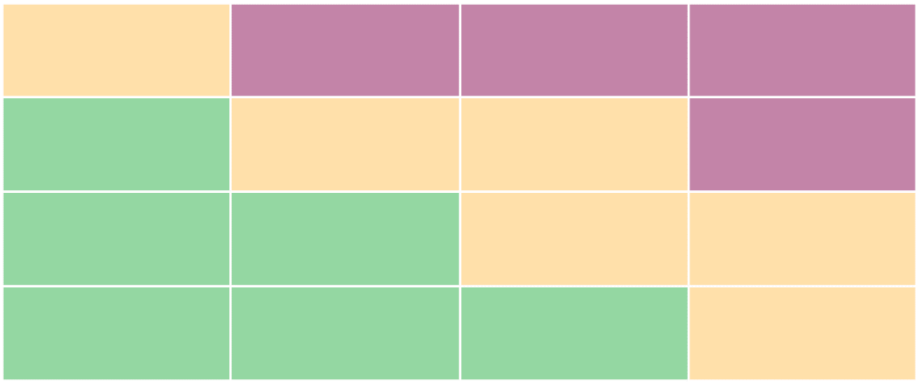
MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO SUL DA BAHIA
PRÓ-REITORIA DE PLANEJAMENTO E ADMINISTRAÇÃO
ASSESSORIA ESPECIAL DE CONTROLE INTERNO

PLANO INSTITUCIONAL DE GESTÃO DE RISCOS E CONTROLES INTERNOS



Itabuna-BA
Novembro/2020

1. OBJETIVO

Este documento tem por objetivo apresentar a metodologia de gerenciamento de riscos, detalhando os processos de gestão de riscos em conformidade com a Política de Gestão de Riscos da Universidade Federal do Sul da Bahia (UFSB), instituída pela Portaria 269, publicada em 10 de maio de 2017.

Neste plano estão descritos os procedimentos a serem utilizados na aplicação da metodologia, papéis e responsabilidades, o referencial teórico, bem como as etapas do processo de gestão de riscos, com finalidade de orientar e gerenciar o modelo de gestão de riscos dos processos e atividades desenvolvidas pelas unidades.

2. APLICABILIDADE

A abrangência deste plano deve ser gradual em todas as Unidades Organizacionais da UFSB, sem prejuízo da utilização de outras normas complementares relativas ao processo de trabalho, projetos ou ações de cada unidade. Este plano tem vigência de cinco anos, com reavaliação anual realizada pelo Comitê de Governança, Gestão de Riscos e Controles Internos (CGRC) e pela Assessoria Especial de Controle Interno.

3. MOTIVAÇÃO E IMPORTÂNCIA DA GESTÃO DE RISCOS

Risco é o efeito da incerteza na consecução dos objetivos de uma organização. São eventos que podem comprometer o alcance das metas institucionais e estão presentes a todo momento, em maior ou menor grau. Se não gerenciados, os riscos podem se materializar e afetar a capacidade de uma organização em gerar valor.

Figura 1 - Benefícios da gestão de riscos.

Por outro lado, a gestão de riscos quando bem implementada possibilita benefícios importantes para a Universidade como o aperfeiçoamento da governança, melhoria do processo de tomada de decisão, otimização dos processos organizacionais, geração de valor público, cumprimento das leis, normas e regulamentos, entre outros.

4. RESPONSABILIDADES

Cada grupo de profissionais e unidades presentes na instituição possuem uma função para que a gestão de riscos seja efetiva. O conjunto de papéis e responsabilidades adotado tem como base a abordagem das Três Linhas de Defesa, que visa comunicar de maneira simples sobre as funções esperadas de cada agente sem sobreposição (TCU, 2018). Ao dirigente máximo compete manter o bom funcionamento das três linhas, dado que estas disponibilizarão informações relevantes e úteis à gestão universitária.

Dessa forma, a primeira linha de defesa diz respeito a todos os agentes públicos que executam diariamente processos/atividades/tarefas relacionadas aos objetivos da Universidade e aplicam os controles primários. Competem a esses agentes:

- Estabelecer as especificidades do contexto para o processo de gestão de riscos.
- Definir os níveis de risco aceitáveis tendo em vista este plano e a política de gestão de riscos.
- Identificar, avaliar, controlar e mitigar riscos nos seus processos de trabalho.
- Monitorar e analisar a evolução do perfil dos riscos mapeados.
- Aplicar as medidas de mitigação necessárias.
- Consultar e comunicar sobre situações que envolvam risco ou mudanças significativas nos processos.
- Disponibilizar informações adequadas quanto à gestão de riscos dos seus processos.

A segunda linha de defesa, situada ao nível da gestão, tem a função de supervisionar as atividades executadas pela primeira linha e também garantir o funcionamento adequado do processo de gestão de riscos. Será desempenhada pelo Comitê de Governança, Gestão de Riscos e Controles Internos e pela Assessoria Especial de Controle Interno. O CGRC é composto pelo Reitor, Vice-Reitor e Pró-Reitores. Competem aos agentes da segunda linha de defesa:

- Aprovar e gerenciar o Plano de Gestão de Riscos.
- Estabelecer os limites de exposição a riscos.
- Determinar medidas mitigadoras, de monitoramento e comunicação das ações.
- Garantir aderência as leis, normas, códigos e outras regulamentações.
- Tomar decisões considerando as informações da gestão de riscos.
- Garantir a disponibilidade da informação em todos os níveis.

Por fim, a terceira linha de defesa é exercida pela Auditoria Interna que avalia de forma independente a eficácia do gerenciamento de riscos e controle interno adotado pela primeira linha e supervisão dos controles desempenhada pela segunda linha, reportando eventuais deficiências e propondo ações de melhorias.

A figura a seguir demonstra as linhas de defesa e o fluxo de informações na Gestão de Riscos na UFSB:

Figura 2 – Linhas de defesa na Gestão de Riscos na UFSB.

5. METODOLOGIA

A metodologia de gerenciamento de riscos é composta por um conjunto de etapas, ferramentas e técnicas para identificar, avaliar, administrar e monitorar os eventos de risco aos quais a Universidade está exposta, de modo que as etapas interagem de forma cíclica, dinâmica e constante.

Os procedimentos para a operacionalização da gestão de riscos na UFSB aderem aos princípios do ForRisco, COSO (*Committee of Sponsoring Organizations of the Treadway Commission*), e boas práticas relacionadas ao tema.

Dessa forma, as etapas do processo de gestão de riscos na UFSB são: definir a política, estabelecer contexto externo, definir estratégia para gestão de riscos, estabelecer contexto interno, gestão dos riscos dos processos, reavaliação da política e avaliação da maturidade.

Figura 3 - Ciclo de gerenciamento de riscos na UFSB.

Segundo o ForRisco, é preciso pensar nas etapas que são genéricas e específicas, bem como nos níveis macro e micro. As ações genéricas são aquelas que envolvem toda a organização. Como específicas, entende-se ações que se referem exclusivamente a uma determinada área dentro do órgão. Por outo lado, atividades de nível macro indica que toda a organização é capaz de receber ou sentir a repercussão destas ações. O nível micro assinala que a repercussão será recebida somente pela área executora. A figura abaixo ilustra a estruturação das etapas.

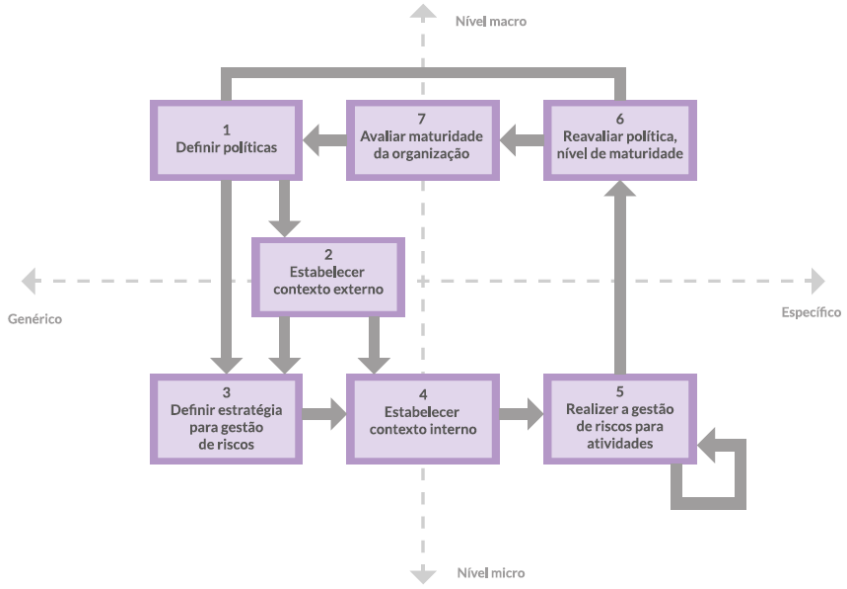


Figura 4 - Ciclo de gestão de riscos ForRisco

Convém destacar que a execução das etapas do ciclo de gestão de riscos pressupõe uma etapa anterior de mapeamento dos processos de trabalho e fixação dos objetivos estratégicos da Universidade. Com o entendimento do fluxo das atividades internas é possível identificar os eventos com potencial de prejudicar o alcance dos objetivos previstos no PDI.

O gerenciamento de riscos deverá ser implementado de forma gradual em todas as áreas da UFSB, sendo priorizados os processos organizacionais que impactam diretamente no alcance dos objetivos estratégicos definidos no PDI. A identificação e priorização desses processos compete ao dirigente máximo da unidade – Pró-Reitoria, Decanatos, Assessorias.

Do exposto, cada etapa do ciclo será detalhada abaixo, com informações a respeito das técnicas a serem aplicadas, o recorte das etapas e os resultados esperados.

5.1 Definição da política de gestão de riscos

A definição da política de gestão de riscos visa estabelecer os princípios, as diretrizes e as responsabilidades envolvidas no gerenciamento de riscos a nível institucional. A política da UFSB foi instituída pela Portaria 34, publicada em 15 de abril de 2020 (https://www.ufsb.edu.br/images/boletins/2020/BS_04_Abril_2020_FINAL_-_2.pdf).

A divulgação da política será intensificada à medida que ocorra o amadurecimento da gestão de riscos na instituição, mediante a execução deste plano, envolvimento da comunidade acadêmica nas oficinas de trabalho, reuniões frequentes dos membros do Comitê e deliberações a respeito da gestão de riscos.

5.2 Estabelecer o contexto externo

Estabelecer o contexto externo passa por entender as leis, normas, códigos, planos, políticas e expectativas das partes interessadas que formam a base para implementar a política de gestão de riscos.

Consiste em reconhecer o ambiente externo onde a Universidade atua na busca de seus objetivos. São situações que estão fora do campo de controle da instituição e, portanto, é importante que sejam consideradas, de modo a evitar ameaças e aproveitar as oportunidades.

Esta etapa é entendida como genérica, tanto de nível macro quanto micro, ou seja, deve ser realizada pelo Comitê e também pelos servidores individualmente, com reflexo no conjunto da instituição e no contexto dos setores.

5.2.1. No nível do Comitê, os membros devem estabelecer o contexto geral que norteia o processo de gestão de riscos, identificando os parâmetros externos que influenciam as atividades de gestão de riscos a nível institucional, considerando cenário atual e futuro, oportunidades e ameaças, percepções das partes interessadas e outros fatos relevantes.

5.2.2. No nível dos setores, os servidores devem estabelecer o contexto externo, considerando os fatores que influenciam o alcance dos objetivos relacionados ao processo organizacional. Para tanto, devem considerar elementos do mapeamento de processos, cenário atual e futuro, oportunidades e ameaças, percepções das partes interessadas e outros fatos relevantes.

5.2.3. Para estabelecer o contexto externo serão utilizadas as técnicas Brainstorming e SWOT, tanto pelo Comitê quanto pelos servidores que atuam diretamente nos processos de trabalho. A primeira ferramenta consiste na reunião dos membros para discutir e listar os elementos do contexto externo. A segunda auxiliará na organização do contexto considerando as oportunidades e ameaças do ambiente externo.

Figura 5 - Ferramenta SWOT

5.2.4. O contexto deverá ser revisado e atualizado juntamente com o ciclo de gestão de riscos.

5.2.4. A saída do processo de análise do contexto deve ser um relato conciso do ambiente externo no qual a instituição/processo se insere, assim como os fatores que podem afetar os resultados – Anexo I Formulário Definição do Contexto.

5.3 Estratégia para a gestão de riscos

A estratégia para a gestão de riscos passa por definir claramente os papéis que formarão as linhas de defesa, com a disposição das obrigações associadas. A estratégia também envolve treinamento das pessoas e à disseminação da gestão de riscos para nivelar o entendimento entre os entes institucionais.

Definir a estratégia para a gestão de riscos é uma atividade comum a toda a organização, mas são executadas também nas unidades da organização, refletindo os seus diferentes contextos.

5.3.1. O Comitê de Governança, Gestão de Riscos e Controles Internos e os servidores devem observar os papéis e responsabilidades do processo de gestão de riscos, conforme o modelo de três linhas de defesa apresentado no tópico 4.

5.3.2. A gestão de riscos será implementada de forma gradual em todas as áreas da Universidade, sendo priorizado os processos organizacionais que impactam diretamente no atingimento dos objetivos estratégicos definidos no Plano de Desenvolvimento Institucional (PDI).

5.3.3. A condução da gestão de riscos é orientada por processos e utilizará os resultados gerados pelo mapeamento dos processos organizacionais como descrição, fluxo, envolvidos e responsáveis, legislações e normas pertinentes, entre outros.

5.3.4. A operacionalização da gestão de riscos ocorrerá mediante oficinas de trabalho com os servidores que conheçam o processo, seus objetivos, contextos, atores envolvidos e controles existentes. As oficinas serão coordenadas pela Assessoria Especial de Controle Interno, visando avaliar os riscos associados aos processos organizacionais.

5.3.5. O treinamento e capacitação dos servidores será realizado com suporte da Assessoria Especial de Controle Interno, no momento das oficinas de trabalho do processo de gestão de riscos. Os treinamentos também podem ser solicitados pelas unidades.

5.4 Estabelecer o contexto interno

Estabelecer o contexto interno significa entender o ambiente interno onde a Universidade atua na busca de seus objetivos. São os pontos fortes e pontos fracos que influenciam a capacidade da Universidade de gerar valor. Portanto, estão no campo de controle da instituição.

Existem alguns fatores do ambiente interno que auxiliam o estabelecimento do contexto, tais como governança, cultura, processos, estrutura e estratégia da organização (Miranda, 2017). Esses elementos apontam para aspectos que ser otimizados e outros que podem ser potencializados.
Esta etapa é genérica, de nível micro e macro, devendo ser realizada pelo Comitê e pelos servidores individualmente. As ferramentas utilizadas serão as mesmas definidas no tópico 5.2.3.

5.3.1. No nível do Comitê, os membros devem estabelecer o contexto geral que norteia o processo de gestão de riscos, identificando os parâmetros internos (planos, normas, regimentos, pontos fortes e fracos) que influenciam as atividades de gestão de riscos a nível institucional.

5.3.2. Para auxiliar o entendimento do contexto interno será utilizado como parâmetro o resultado do processo de avaliação da maturidade da instituição, quanto aos aspectos de estratégia, governança, política, processos, linguagem e métodos de avaliação, sistemas e dados, comunicação e cultura.

5.3.3. No nível dos setores, os servidores devem estabelecer o contexto interno que influencia nos objetivos relacionados ao processo organizacional, considerando políticas, objetivos e estratégias que o impactam, forças e fraquezas, percepções das partes interessadas, e outros fatos relevantes.

5.3.4. Nesta etapa deve ser discutido e avaliado o apetite a risco da Universidade. Oportunamente, as unidades também devem analisar o apetite e tolerância a risco para o processo organizacional.

5.3.4. A saída do processo de análise do contexto deve ser um relato conciso do ambiente interno no qual a instituição/processo se insere, assim como os fatores que podem afetar os resultados – Anexo I Formulário Definição do Contexto.

5.5 Gestão dos riscos dos processos

A gestão dos riscos dos processos envolve as subetapas de i) identificação e análise, ii) avaliação, iii) tratamento, iv) monitoramento e análise crítica e v) comunicação e consulta. Essas

etapas são específicas e de nível micro, portanto, devem ser seguidas por todos os servidores quando do gerenciamento de riscos.

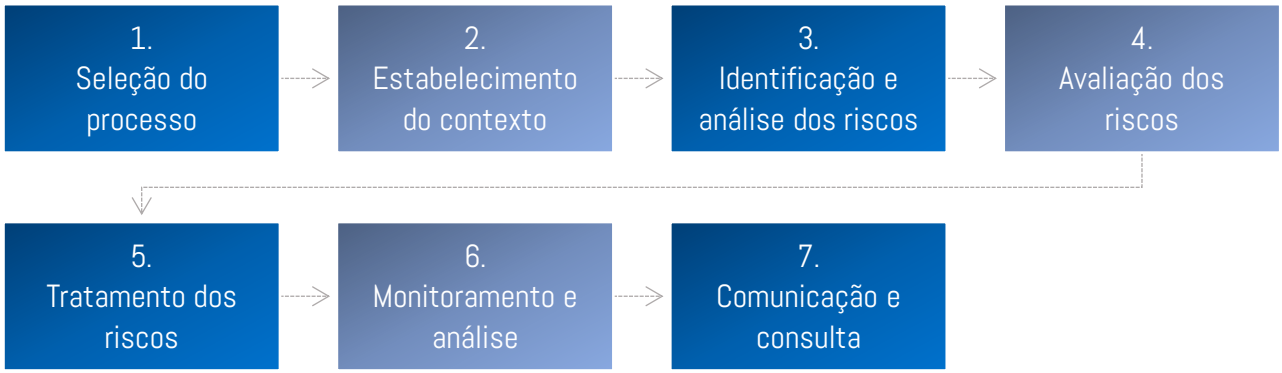


Figura 6 – Gestão de riscos dos processos.

5.5.1 Identificação dos riscos

Consiste em buscar, identificar, descrever e analisar eventos de risco que afetam a realização dos objetivos de um processo organizacional. Esta etapa tem como finalidade produzir uma lista abrangente de riscos, mesmo aqueles provenientes do ambiente externo, dado que se o risco não for identificado nesta etapa, ele não pode ser analisado ou tratado (CFC, 2017).

A identificação deve analisar os eventos de riscos, suas fontes e causas e potenciais consequências que podem evitar, atrasar, prejudicar ou impedir o cumprimento dos objetivos, tendo em vista o contexto anteriormente estabelecido.

5.5.1.2. Com base no mapeamento de processos, os servidores devem identificar os eventos de risco que ameaçam o processo organizacional, e classificá-los quanto à sua origem e categoria:

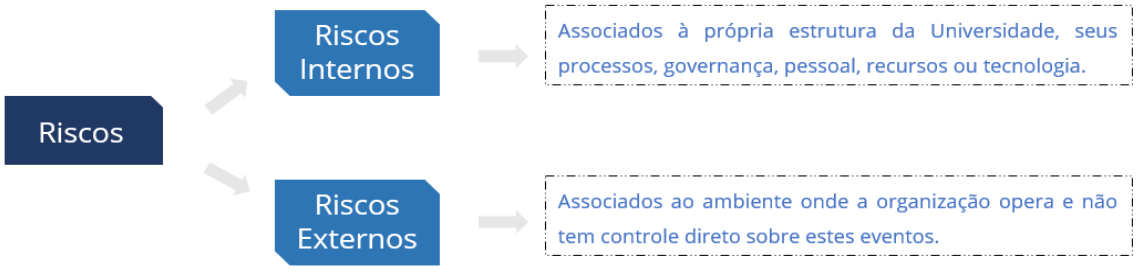


Figura 7 - Classificação quanto a origem dos riscos.

Tipos de Risco	Descrição
Operacionais	Possibilidade de ocorrência de eventos que podem comprometer as atividades do órgão ou da instituição, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestruturas e sistemas.

Legal & Conformidade	Possibilidade de ocorrência de eventos relacionados ao cumprimento da legislação e/ou regulamentação externa e às normas e procedimentos internos.
Integridade	Eventos que podem afetar a probidade da gestão dos recursos públicos e das atividades da organização, causados pela falta de honestidade e desvios éticos.
Financeiros & Orçamentários	Possibilidade de ocorrência de eventos que podem comprometer a capacidade do órgão ou da instituição de contar com recursos orçamentários e financeiros necessário à realização de suas atividades, ou de eventos que possam comprometer a própria execução orçamentaria, tais como atrasos no cronograma de licitações.
Imagem & Reputação	Possibilidade de ocorrência de eventos que podem comprometer a confiança da sociedade (ou de parceiros, clientes ou de fornecedores) em relação à capacidade do órgão ou da instituição em cumprir a missão institucional.
Político	Possibilidade de ocorrência de eventos externos relacionados a mudanças e decisões políticas que podem comprometer as atividades da organização.
Ambiental	Possibilidade de ocorrência de eventos que possam provocar danos ambientais causados pelas atividades da organização ou devido a ocorrência externa.
Tecnologia	Eventos relacionados ao desenvolvimento tecnológico, acesso as inovações e disponibilidade de ferramentais, materiais e internet.
Recursos Humanos	Eventos que possam comprometer o provimento de servidores necessários à realização das atividades da organização.
Infraestrutura & Logística	Eventos que possam comprometer o provimento de recursos e espaços para a execução de todas as atividades da organização.

Figura 8 - Classificação quanto aos tipos de riscos, adaptado da Unifal e CGU.

5.5.1.4. Cada risco identificado deve ser atribuído ao "proprietário do risco", responsável por assegurar as atividades de gestão de riscos.

5.5.1.4. A identificação dos riscos seguirá uma abordagem de autoavaliação, na qual cada segmento revê suas atividades e contribui para o diagnóstico da situação. Essa autoavaliação será mediada pela Assessoria de Controle Interno, através de oficinas de trabalho.

5.5.1.5. As técnicas de "brainstorming" e "bow tie" serão utilizadas para auxiliar na identificação dos riscos. Brainstorming permite reunir pessoas conhecedoras de certa atividade da instituição e incentivar o fluxo livre de conversação entre elas, com o objetivo de identificar possíveis eventos de riscos. Por outro lado, a bow tie (gravata borboleta) busca analisar e

descrever os caminhos de um evento de risco, desde suas causas até as consequências, por meio de uma representação gráfica (TCU, 2018).

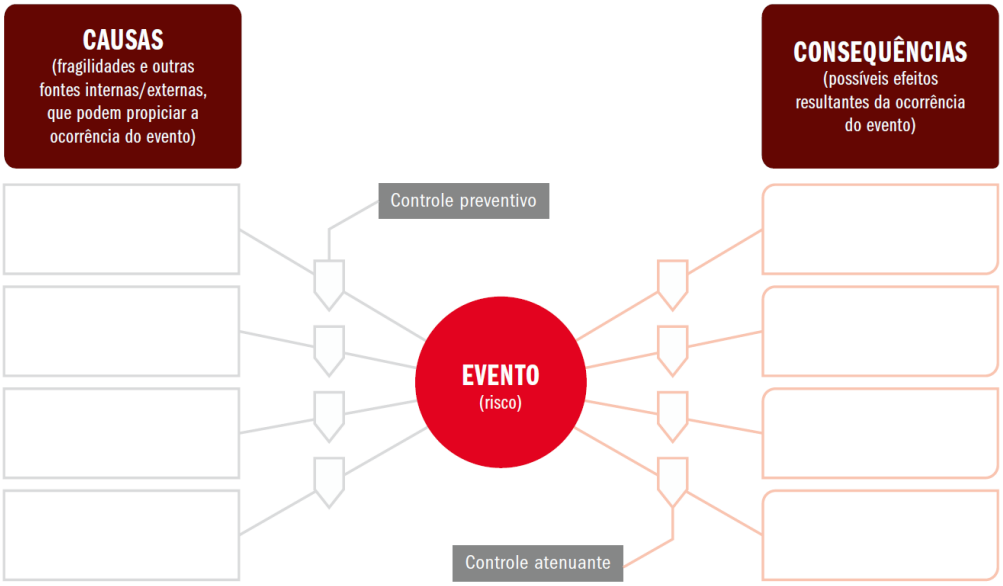


Figura 9 - Representação gráfica do diagrama "bow tie" (TCU).

5.5.1.3. Os riscos devem ser registrados no Anexo II – Formulário de Identificação de riscos.

5.5.2 Avaliação de riscos

A finalidade da avaliação de riscos é auxiliar na tomada de decisões, com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento e a prioridade para implementar o tratamento. Envolve comparar nível de risco com os critérios de risco estabelecidos quando o contexto foi considerado, para determinar se o nível de risco é aceitável ou se algum tratamento é exigido (ABNT, 2009).

Conforme o TCU (2018) e CFC (2017), compõem os critérios de risco:

⏩ Escala de probabilidade: define como a probabilidade será medida. Está associada à chance de ocorrência de um evento de risco.

⏩ Escala de impacto: Define as consequências dos eventos de riscos, considerando seus efeitos perante os objetivos e a sua capacidade de recuperação. Desse modo, para a definição do nível de impacto, é necessário primeiro considerar os objetivos do processo de trabalho analisado.

⏩ Matriz Impacto X Probabilidade: define como o nível de risco inerente e residual deve ser determinado.

⏩ Matriz Apetite a Risco: relaciona o nível em que um risco se torna aceitável ou inaceitável pela Universidade.

⏩ Matriz Classificação de Riscos: categoriza os riscos definidos na Matriz Probabilidade X Impacto como "Extremo", "Alto", "Médio" e "Baixo".

⏩ Diretrizes para priorização e tratamento: determina a diretriz, a resposta ao risco, o plano de ação, responsáveis e o cronograma de execução.

⏩ Eficácia dos controles: critério utilizado para cálculo do risco residual, o qual analisa a situação do controle existente quanto a sua implementação, abrangência e eficiência. Os controles podem ser categorizados como "Inexistente", "Fraco", "Mediano" e "Forte".

⏩ Risco Inerente: risco intrínseco a natureza do processo, desconsiderando qualquer controle existente.

⏩ Risco Residual: risco do processo que permanece mesmo após o tratamento ou medida adotada para controlar o risco.

5.5.2.1. Os riscos devem ser classificados quanto a sua probabilidade de ocorrência e quanto ao impacto. A probabilidade varia entre muito baixa, baixa, média, alta e muito alta. O impacto tem a escala de muito baixo, baixo, médio, alto e muito alto.

5.5.2.2. Inicialmente será calculado o Risco Inerente (RI), aquele que desconsidera qualquer ação de mitigação/controle do risco. O nível de risco inerente é obtido pela combinação entre a Probabilidade (P) e o Impacto (I).

Risco = P x I

5.5.2.3. Na avaliação da probabilidade do evento de risco, o servidor deverá considerar a seguinte escala de probabilidade:

PROBABILIDADE	DESCRIÇÃO DA PROBABILIDADE, DESCONSIDERANDO OS CONTROLES	FREQUÊNCIA	PESO
Muito baixa	**Improvável**. Em situações excepcionais, o evento pode até ocorrer, mas nada nas circunstâncias indica essa possibilidade. Este evento pode ter acontecido anteriormente na organização. Entretanto, na ausência de outras informações ou circunstâncias excepcionais, **não seria esperado** que ocorresse na organização no futuro próximo.	<10%	1
Baixa	**Rara**. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade. O evento não ocorre de maneira frequente na organização. Os controles atuais e as circunstâncias sugerem que a ocorrência seria considerada **altamente não usual**.	>10% <=30%	2
Média	**Possível**. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade O evento pode ter ocorrido ocasionalmente na organização. Os controles atuais ou as circunstâncias sugerem que **há uma possibilidade plausível** de ocorrência.	>=30% <=50%	3
Alta	**Provável**. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade. Este evento pode ocorrer regularmente na organização. Com os controles atuais ou circunstâncias, **pode-se esperar que ocorra** ao longo de 1 ano.	>50% <=90%	4
Muito alta	**Praticamente certa**. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade Este evento ocorre frequentemente na organização ou com os controles ou circunstâncias **espera-se sua ocorrência**.	>90%	5

Figura 10 - Escala de probabilidade. Fonte: Adaptado do documento Avaliação de Maturidade, TCU, 2018.

5.5.2.4. Na avaliação do impacto, o servidor deverá considerar a seguinte escala de consequências:

	ÁREAS DE IMPACTO				
NÍVEL	**ABRANGÊNCIA**	**DESEMPENHO OPERACIONAL**	**LEGAL & CONFORMIDADE**	**IMAGEM & REPUTAÇÃO**	**ORÇAMENTÁRIO**
	Impacta na instituição inteira ou somente algumas unidades?	*Interrompe as operações ou de entrega de produtos/serviços?* *Afeta projetos, programas ou ações?*	*Viola leis, normas ou procedimentos?* *Pode resultar em litígios ou multas?*	*Afeta a imagem da Universidade?* *Traz exposição na mídia?* *Quem representa a Universidade frente a mídia?*	*Afeta o orçamento institucional?* *Compromete a sustentabilidade financeira?*
1. Muito baixo	Impacto mínimo. Apenas um setor é afetado	Impacto mínimo nas operações ou resultados dos processos. Não compromete o alcance dos objetivos propostos. Regularização rápida pela equipe interna através da revisão de processos de trabalho.	Não afeta a conformidade com a legislação, regulação vigente ou procedimentos internos.	Apenas o setor envolvido toma conhecimento. Gera pouca preocupação interna. Sem cobertura ou exposição na mídia.	Impacto mínimo no orçamento institucional, recuperável no exercício financeiro atual
2. Baixo	Vários setores da mesma unidade organizacional são afetados	Pode ocorrer alguma interrupção nas operações ou resultados dos processos. Regularização rápida pela equipe interna (em até um mês)	Resulta em questões legais menos complexas. Afeta pouco as questões de legislação/regulação, mas que podem, eventualmente, ser tratadas pela Procuradoria Jurídica.	Apenas os envolvidos tomam conhecimento. Pode ocorrer algum impacto de imagem na comunidade interna. Eventual atenção e exposição negativa na mídia local.	Impacto pequeno, mas perceptível, no orçamento institucional, recuperável no exercício financeiro atual
3. Médio	Uma unidade organizacional inteira é afetada	Ocorre interrupção nas operações ou resultados dos processos, com impacto no fluxo de trabalho. Requer priorização da unidade para regularizar a situação.	Afeta a conformidade de legislação/regulação, resulta em incidente sério, com possível investigação e avaliação sobre responsabilidade legal.	Atenção e exposição negativa na mídia (dias) e gera preocupação interna. Pode levar a perda de confiança na instituição. Gera preocupação interna da alta gestão.	Impacto alto no orçamento institucional, recuperável no exercício financeiro atual, mas requer priorização
4. Alto	Várias unidades organizacionais são afetadas	Ocorre interrupção severa nas operações ou resultados dos processos, com impacto negativo na imagem da Universidade. Requer priorização da alta gestão para regularizar a situação.	Resulta em violações graves de legislação e regulação vigente. Pode envolver litígios que requeiram forte envolvimento da Procuradoria Jurídica	Atenção e exposição negativa e prolongada na mídia (semanas). Leva a perda de confiança na instituição. Requer foco total da alta gestão para regularizar a situação.	Impacto muito alto no orçamento institucional, não recuperável no exercício financeiro atual, nem no próximo
5. Muito alto	Toda a Universidade é afetada	Ocorre interrupção completa nas operações ou resultados dos processos por período indeterminado, exigindo intervenção da alta administração para regularizar a situação.	Resulta em violações graves de legislação e regulação vigente. Resulta em litígios e multas significativas. Pode envolver atividades sindicais.	Atenção extremamente negativa e prolongada da mídia (meses). Leva a perda de confiança irreconciliável. Requer foco total da alta gestão para regularizar a situação.	Impacto crítico de longo prazo no orçamento institucional, não recuperável no exercício financeiro atual, nem no próximo

Figura 11 - Escala de impacto. Fonte: adaptado da Avaliação de Maturidade (TCU, 2018) e Manual de Riscos da ANS.

5.5.2.5. O resultado da combinação entre probabilidade x impacto deve ser expresso no Mapa de Riscos, a seguir.

IMPACTO						
	Muito Alto 5	5 RM	10 RM	15 RA	20 RE	25 RE
	Alto 4	4 RB	8 RM	12 RA	16 RA	20 RE
	Médio 3	3 RB	6 RM	9 RM	12 RA	15 RA
	Baixo 2	2 RB	4 RB	6 RM	8 RM	10 RM
	Muito Baixo 1	1 RB	2 RB	3 RB	4 RB	5 RM
		Muito Baixa 1	Baixa 2	Média 3	Alta 4	Muito Alta 5
		PROBABILIDADE				

Figura 122 – Matriz de riscos. Fonte: adaptado da Avaliação de Maturidade (TCU, 2018).

5.5.2.6. Posterior à avaliação do risco inerente, a equipe técnica deve identificar a existência e eficácia dos controles internos adotados pelos servidores para tratar os riscos. Os controles levantados serão classificados conforme sua eficácia, ou Nível de Confiança (NC), de acordo com a escala do TCU, a seguir.

NÍVEL DE CONFIANÇA	DESCRIÇÃO (DESENHO E IMPLEMENTAÇÃO)	RISCO DE CONTROLE
Inexistente	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	Muito Alto 1
Fraco	Controles informais, depositados na esfera de conhecimento pessoal dos operadores do processo, tendem a ser aplicados caso a caso, em geral realizados de maneira manual.	Alto 0,8
Mediano	Controles parcialmente implementados, mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes devido a deficiências no desenho ou nas ferramentas utilizadas.	Médio 0,6
Satisfatório	Controles formalmente desenhados, implementados e sustentados por ferramentas adequadas e, embora passiveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	Baixo 0,4
Forte	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco. São periodicamente testados, revisados e aperfeiçoados.	Muito Baixo 0,2

Figura 1313 – Nível de confiança dos controles internos. Fonte: Avaliação de Maturidade (TCU, 2018) e Manual de Riscos da ANS.

5.5.2.7. Determinado o nível de confiança dos controles, é possível estimar o Risco Residual (RR), ou seja, aquele que permanece mesmo após as ações de controle ao risco. O cálculo do RR é o produto da multiplicação entre o risco inerente e o fator de risco de controle.

RR = RI X RC

RR = nível do risco residual

RI = nível do risco inerente

RC = risco de controle

5.5.2.8. O resultado do risco residual pode fazer com que o risco se enquadre em uma faixa de classificação diferente definida para o risco inerente.

5.5.2.9. A escala do risco residual varia entre risco baixo, risco médio, risco alto e risco extremo.

RB (Risco Baixo)	RM (Risco Médio)	RA (Risco Alto)	RE (Risco Extremo)
1 - 4	5 - 11	12 - 19	20 - 25

5.5.2.1.1. O nível de criticidade do risco será avaliado considerando a Matriz de Apetite a Risco, a qual define a quantidade de risco que a Universidade está disposta a aceitar para alcançar seus objetivos institucionais e gerar valor à sociedade. Cabe apenas ao Comitê alterar esta matriz.

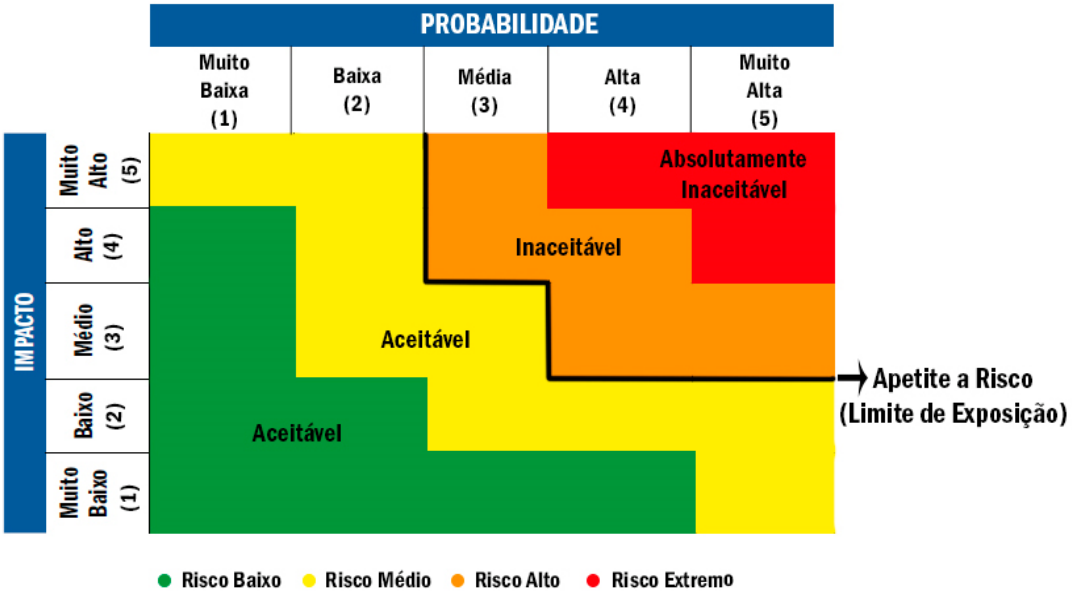


Figura 14 - Matriz de apetite a risco da UFSB.

5.5.2.1.2. O resultado da avaliação de risco deve apontar para riscos que necessitam ser tratados com prioridade em relação a outros, considerando o nível de risco. Se o risco é igual ou inferior ao nível de aceitação, esse risco é considerado aceitável, mantendo os tratamentos atuais. No entanto, se o nível do risco residual é superior ao apetite admitido pela Universidade, então esse risco demandará ação adicional em seu tratamento, a fim de reduzi-lo a um nível aceitável (CFC, 2017).

5.5.2.1.3. A probabilidade e o impacto dos riscos devem ser registrados no Anexo III – Formulário de Avaliação de riscos.

5.5.3. Tratamento de riscos

O tratamento dos riscos consiste em selecionar uma ou mais opções para modificar o nível do risco (a probabilidade ou o impacto) e a elaboração de planos de tratamento dos riscos avaliados

na etapa anterior. Estes planos podem implicar na introdução de novos controles ou modificar os existentes (ABNT, 2009).

A pontuação dada pela matriz de riscos (apresentada no tópico acima) possibilita organizar os riscos em nível de criticidade, resultado em uma ordem de priorização: quanto maior a pontuação, mais crítico e, portanto, maior prioridade deve ser dada ao seu tratamento/gerenciamento.

5.5.3.1. Conforme o Tribunal de Contas da União, as opções de tratamento dos riscos envolvem evitar, reduzir, transferir ou aceitar o risco.

- Evitar: eliminar a fonte do risco, intervindo diretamente nas causas do risco. Também pode envolver a decisão de não iniciar ou continuar a atividade, parar o processo operacional.

- Reduzir ou mitigar: adotar medidas para reduzir a probabilidade e/ou impacto dos riscos.

- Compartilhar: consiste em transferir o risco ou parte dele com outras partes.

- Aceitar: não adotar nenhuma medida para alterar a probabilidade e/ou impacto dos riscos. Indica que o risco está dentro do apetite a risco da Universidade, que o custo de adotar um controle é superior ao benefício gerado ou que não é possível adotar nenhuma ação.

5.5.3.2. Com base na resposta selecionada, será elaborado um plano de ação para tratamento dos riscos que deve considerar:

- A eficácia das ações já existentes.
- As restrições organizacionais, técnicas e estruturais.
- Os requisitos legais.
- A análise custo/benefício.
- As ações a serem realizadas.
- Os responsáveis.
- As prioridades.
- O cronograma de execução.

5.5.3.3. Cada risco associado ao processo deve receber uma opção de tratamento. A escolha da opção depende do nível do risco, contexto interno ou custo do controle, conforme apresenta o quadro abaixo.

Tabela 1 - Opções de tratamento do risco.

NÍVEL DE RISCO	DESCRIÇÃO	AÇÃO NECESSÁRIA	RESPOSTA
EXTREMO	Nível de risco **muito além do apetite a risco** da Universidade, absolutamente inaceitável.	Riscos encontrados nessa faixa devem ser comunicados ao Comitê de Gestão de Riscos, à Assessoria de Controle Interno e ao dirigente máximo da unidade. Devem possuir plano de mitigação e contingência imediatamente. Postergação de medidas só com autorização do dirigente máximo.	Mitigar Evitar Compartilhar
ALTO	Nível de risco inaceitável, **além do apetite a risco** da Universidade.	Riscos encontrados nessa faixa devem ser comunicados ao dirigente máximo da unidade e ter uma ação tomada em período determinado. Devem possuir plano de mitigação e contingência imediatamente. Postergação de medidas só com autorização do dirigente da área.	Mitigar Evitar Compartilhar
MÉDIO	Nível de risco **dentro do apetite a risco** da Universidade.	Geralmente nenhuma ação especial é necessária, porém requer atividades de monitoramento e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-los sem custos adicionais. Deve possuir uma ação de contingência associada ao risco.	Aceitar
BAIXO	Nível de risco **dentro do apetite** a risco da Universidade.	Monitorar o perfil do risco. É possível que existam oportunidades de maior retorno que podem ser exploradas, assumindo-se mais riscos, avaliando a relação custo x benefício, como diminuir o nível de controles. Deve possuir uma ação de contingência associada ao risco.	Aceitar

Fonte: Avaliação de maturidade TCU e CGU 2018.

5.5.3.4. Se a opção de tratamento for mitigar, devem ser definidas medidas de tratamento para esse risco. Essas medidas devem ser capazes de diminuir os níveis de probabilidade e/ou impacto do risco a um nível dentro ou mais próximo possível das faixas de apetite a risco (risco baixo ou médio).

5.5.3.5. A escolha por evitar o risco deve ser avaliada individualmente pelo Comitê de Governança, Gestão de Riscos e Controles Internos, uma vez que podem implicar no encerramento de um importante serviço/atividade que o poder público presta (Miranda, 2017).

5.5.3.6. A seleção da opção compartilhar o risco deve ser avaliada individualmente pelo Comitê de Gestão de Riscos, Controles Internos e Governança, dado que resulta na transferência de responsabilidade.

5.5.3.7. Se a opção de tratamento for aceitar o risco, deve ser elaborado um plano de contingência para o caso do risco se concretizar.

5.5.3.8. A responsabilidade pelo plano de tratamento é da unidade organizacional responsável pelo processo organizacional. No plano de ação deve ser definido o principal responsável pela implementação (servidor ou cargo), que também deverá monitorar e reportar a evolução das ações.

5.5.3.9. Se o plano envolver mais de uma unidade, o responsável pelo processo de gerenciamento do risco deve encaminhar a proposta do plano para que as demais unidades validem as iniciativas.

5.5.3.1.1. O plano de ação deve ser registrado no Anexo IV – Formulário de Tratamento de riscos.

5.5.4. Monitoramento e análise crítica

O monitoramento e análise crítica constituem uma importante etapa do ciclo de gestão de riscos, uma vez que os objetivos de uma organização podem mudar, assim como o contexto e as incertezas enfrentadas.

O mapa de risco será a principal ferramenta de monitoramento do processo de gerenciamento de riscos e controles internos da unidade.

5.5.4.1. Os riscos associados aos processos da Universidade devem ser monitorados e analisados sistematicamente pelo respectivo dono do processo com a finalidade de:

- identificar mudanças no perfil do risco e ajustar resposta.
- detectar mudanças no contexto externo e interno.
- obter informações adicionais para aprimorar a política e o processo de gestão de riscos.
- analisar eventos, mudanças, tendências, sucessos e fracassos, para aprender com eles.
- identificar riscos emergentes, que poderão surgir após o processo de análise crítica
- garantir que os controles sejam eficazes e eficientes no projeto e operação (ABNT, 2009).

5.5.4.2. São responsáveis pela realização desta etapa:

- Proprietário do risco: são, em geral, os Pró-Reitores, Decanos, Chefe de Gabinete e Assessores. Suas atribuições compreendem assegurar que os riscos sejam monitorados, gerenciados e tratados adequadamente no âmbito de sua unidade organizacional.

  Devem agregar as informações dos gestores de riscos mediante relatório anual de riscos, a ser repassado para o Comitê de Governança, Gestão de Riscos e Controles Internos, demonstrando a execução dos planos de ação. Os riscos classificados como “alto” e “extremo” devem ser monitorados continuamente e relatados a cada seis meses ao Comitê de Governança, Gestão de Riscos e Controles Internos.

- Gestor do risco: são os servidores, coordenadores, diretores, chefes de setores e seções, responsáveis por processos organizacionais. São responsáveis por executar as atividades de gestão de riscos e coordenar esforços para identificar e estimar riscos, bem como propor melhorias necessárias para mitigar riscos, além de comunicar os resultados a todos os interessados.

  Devem elaborar relatório anual das ocorrências de riscos e da eficiência dos controles adotados. Os riscos classificados como “alto” e “extremo” devem ser monitorados

continuamente e relatados a cada seis meses ao Comitê de Governança, Gestão de Riscos e Controles Internos.

- Comitê de Governança, Gestão de Riscos e Controles Internos: realiza semestralmente o monitoramento e análise crítica de todos os riscos classificados como "altos" e "extremos", ou seja, fora do apetite a risco da Universidade.

  O comitê realizará o monitoramento com base na matriz de riscos e nos relatórios setoriais sobre os planos de tratamento dos riscos.

- Assessoria Especial de Controle Interno: fornece suporte ao monitoramento e análise crítica realizado pelas as unidades organizacionais e comitê, com especial atenção aos riscos "altos" e "extremos". Os riscos baixos e médios devem ser monitorados no sentido de mantê-los nessa condição ou até mesmo explorar potenciais oportunidades.

5.5.4.3. O monitoramento será contínuo e também mediante revisões periódicas específicas. O monitoramento contínuo é aquele realizado nas operações cotidianas da Universidade, incluindo ações que os servidores executam ao cumprir suas responsabilidades. Por outro lado, o monitoramento por revisões periódicas consiste na avaliação anual (semestral, no caso de riscos altos e extremos) submetida ao Comitê de Governança, Gestão de Riscos e Controles Internos.

5.5.4.4. Compete ao proprietário do risco e gestor do risco realizarem o monitoramento contínuo dos eventos de risco, de modo a acompanhar os indicadores de risco, analisar as operações e fluxos de atividades em comparação com os critérios de risco. Ademais, devem realizar a analisar crítica dos riscos e seus tratamentos, por meio de autoavaliação de riscos e controles.

5.5.4.5. Compete à Assessoria Especial de Controle Interno realizar o monitoramento contínuo dos riscos classificados como "alto" e "extremo", auxiliando os servidores na análise crítica dos riscos e os tratamentos adotados. O registro deve ser feito em relatório de progresso de riscos.

5.5.4.6. Mudanças identificadas durante o monitoramento devem ser comunicadas à Assessoria Especial de Controle Interno, a quem compete supervisionar os resultados do processo de gestão de riscos.

5.5.4.7. O registro do tratamento dos riscos deve ser feito no Anexo V – Formulário para Monitoramento e Análise Crítica.

5.5.5. Comunicação e consulta

A comunicação objetiva garantir um fluxo constante de informações com as partes interessadas, internas e externas, durante todas as fases do processo de gestão de riscos, de modo a compartilhar e obter informações relevantes. Esta etapa contribui para outros benefícios, tais como:

- Facilitar a troca de informações relevantes, verdadeiras, exatas e íntegras.
- Comunicar os objetivos e estratégias da Universidade.
- Informar às partes interessadas as responsabilidades em todos os níveis.
- Apoiar todas as atividades do processo de gestão de riscos.
- Melhoria contínua do processo de gestão de riscos (ABNT, 2009).

5.5.5.1. Todos os gestores de riscos são responsáveis por garantir que novos riscos sejam identificados e monitorados, além de comunicá-los aos proprietários de risco, à Assessoria Especial de Controle Interno e ao Comitê de Governança, Gestão de Riscos e Controles Internos, em caso de riscos altos e extremos.

5.5.5.2. Ao comitê compete garantir o acesso às informações sobre os riscos aos quais a Universidade está exposta, sugerindo melhorias no processo de tomada de decisão e ampliação das possibilidades de alcance dos objetivos

5.5.5.3. A comunicação dos riscos deve ser feita no Anexo VI – Formulário para Comunicação de Riscos. Outros formulários e meios de comunicação podem ser criados sem prejuízo das atividades.

5.5.5.4. A comunicação será suportada por um sistema de informação para proporcionar um fluxo de informações indispensáveis ao sucesso das ações de gestão de riscos.

5.5.5.5. Cada unidade deve desenvolver um relatório anual de riscos e controles internos, voltado para comunicar as partes interessadas. O relatório deve conter minimamente as seguintes seções: introdução, estrutura organizacional da unidade, metodologia aplicada, documentos de referência, gestão de riscos e controles, avaliação de riscos e ações de controles propostas, considerações finais e anexos.

6. REAVALIAR A POLÍTICA DE GESTÃO DE RISCOS

A política de gestão de riscos consiste em uma declaração de intenções e diretrizes relacionadas ao gerenciamento de riscos, estabelecendo claramente os objetivos e responsabilidades para tratar o tema no âmbito interno da instituição.

Reavaliar a política significa entender o estágio atual da gestão de riscos, a legislação e eventuais alterações e identificar o nível de maturidade, realinhando ações e práticas relacionadas a gestão de riscos.

6.1. A política de gestão de riscos da UFSB será reavaliada a cada doze meses pelo Comitê de Governança, Gestão de Riscos e Controles Internos, com possibilidade de ser revisada antes desse ciclo, caso o comitê avaliar necessário.

6.1. A reavaliação da política utilizará a técnica de “brainstorming”, garantindo a participação efetiva dos membros do CGRC.

6.2. A reavaliação da política deverá ser registrada em documento específico, com relato conciso a respeito da avaliação realizada e eventuais alterações sugeridas.

7. AVALIAR O NÍVEL DE MATURIDADE

Avaliar o nível de maturidade significa compreender o estágio atual da Universidade quanto ao seu processo de gestão de riscos, visando o autoconhecimento da organização.

7.1. A avaliação da maturidade será conduzida pelo Comitê de Governança, Gestão de Riscos e Controles Internos, com suporte da Assessoria Especial de Controle Interno.

7.2. A mensuração da maturidade considerará os seguintes componentes, definidos na metodologia do Instituto Brasileiro Governança Corporativa (IBGC): (1) estratégias; (2) governança; (3) política; (4) processos, interação dos processos e ciclos de gestão; (5) linguagem e métodos de avaliação; (6) sistemas, dados e modelos de avaliação; (7) cultura, comunicação e treinamento, monitoramento e melhoria contínua.

7.3. Conforme o modelo do IBGC, os níveis de maturidade variam entre:

NÍVEL DE MATURIDADE	DESCRIÇÃO
(1) Inicial	Uma organização que não sabe como, onde e por que implementar a gestão de riscos.
(2) Fragmentado	A organização sabe por onde começar, mas não sabe aonde quer chegar.
(3) Definido	A organização tem objetivos, metas e estratégias definidas.
(4) Consolidado	A organização tem objetivos, metas e estratégias definidas, implementados e monitorados.
(5) Otimizado	A estratégia de gestão de riscos foi revisitada e está claramente definida, implementada e integrada aos demais ciclos de gestão.

Fonte: ForRisco, 2018.

7.4. A metodologia do IBGC será materializada mediante um questionário para avaliação da maturidade – Anexo VI Formulário de Avaliação da Maturidade.

8. SOLUÇÃO TECNOLÓGICA

Nos tempos atuais torna-se imprescindível uma ferramenta tecnológica para auxiliar a implementação do processo de gestão de riscos. Nesse sentido, para acompanhar a gestão de riscos a nível institucional, teremos o apoio do software ForRisco, gratuito e de código aberto, desenvolvido pelo Fórum Nacional de Pró-Reitores de Planejamento e de Administração das Instituições Federais de Ensino Superior – Forplad.

Dentre as principais funcionalidades do software destacam-se a possibilidade de estabelecer o plano de gestão de riscos, suporte para o registro dos riscos, identificação das causas e consequências, definir ações corretivas, indicar periodicidade de análise do risco, apoio ao monitoramento de riscos e a geração de relatórios dinâmicos, entre outras.

O software ForRisco deverá ser utilizado por todos os servidores da Universidade nas etapas do ciclo de gerenciamento de riscos, em conjunto com os demais formulários mencionados ao longo deste plano.

9. VALIDAÇÃO DAS ETAPAS DO CICLO DE GERENCIAMENTO DE RISCOS

Os resultados das etapas anteriores do processo de gerenciamento de riscos devem ser avaliados e aprovados pelo dirigente máximo da unidade organizacional. Após a aprovação desses resultados, o responsável pelo processo de gerenciamento de riscos deve incluir essas informações no software ForRisco e encaminhar esses resultados à Assessoria Especial de Controle Interno, incluindo as iniciativas previstas no Plano de Tratamento dos Riscos.

Para os riscos de nível “extremo” e “alto”, os resultados da gestão de riscos devem ser encaminhados também ao Comitê de Governança, Gestão de Riscos e Controles Internos, que deve validar as iniciativas contidas no plano de tratamento dos riscos.

10. INDICADORES DE DESEMPENHO

Os indicadores são instrumentos fundamentais para medir o desempenho do plano de gestão de riscos, permitindo o monitoramento e análise dos resultados, assim como a tomada de ações corretivas e/ou preventivas visando otimizar as ações. Os indicadores devem apontar para informações pertinentes, oportunas e precisas.

Abaixo alguns indicadores que serão utilizados para acompanhar a execução do plano de gestão de riscos.

ID	INDICADOR	FÓRMULA
01	% Setores da unidade aderentes ao plano	Setores da unidade aderentes ao plano / Total de setores da unidade
02	% Processos mapeados por unidade	Processos mapeados / Total de processos da unidade
03	% Processos críticos mapeados por unidade	Processos críticos mapeados / Total de processos críticos
04	% Processos críticos com riscos mapeados por unidade	Processos críticos com riscos mapeados / Processos críticos
05	% Controle implementados por processo	Controles concluídos / Total de controles do processo

ANEXO I – DEFINIÇÃO DO CONTEXTO

- **UNIDADE**:
- **SERVIDOR**:
- **PROCESSO DE TRABALHO**:
- **OBJETIVO DO PROCESSO DE TRABALHO:**
- **PROPRIETÁRIO DO PROCESSO**:
- **OBJETIVO ESTRATÉGICO RELACIONADO**:
- **DATA DA ANÁLISE**:

LEIS E REGULAMENTOS
Exemplo: Lei 8.112/1990; Portaria 15/2018.

SISTEMAS UTILIZADOS
Exemplo: SIGEPE/SIAFI/SCDP/SIASG.

OBJETIVO ESTRATÉGICO ASSOCIADO
Exemplo: Objetivo 4 – Modernizar a gestão administrativa

ANÁLISE DO AMBIENTE INTERNO	
Forças (Pontos Fortes)	1. Exemplo: Recursos Humanos
	2. Exemplo: Planejamento estratégico
Fraquezas (Pontos Fracos)	1. Exemplo: Disponibilidade financeira
	2. Exemplo: Regulamentação interna
ANÁLISE DO AMBIENTE EXTERNO	
Oportunidades (Pontos Fortes)	1. Exemplo: Nova legislação
	2. Exemplo: Fonte de financiamento
Ameaças (Pontos Fracos)	1. Exemplo: Conjuntura política
	2. Exemplo: Fornecedores

RELATO CONCISO DO CONTEXTO
Exemplo: responder às perguntas direcionadoras abaixo.

PERGUNTAS DIRECIONADORAS

Para auxiliar na definição do contexto de atuação, fazer as seguintes perguntas:

1. Quais objetivos pretende-se alcançar?
2. Quais são as leis, normas e regulamentação que devem ser cumpridas?
3. Quais os pontos fortes e fracos do ambiente interno?
4. No ambiente interno, quais principais planos, políticas e estratégias e diretrizes que impactam o processo?
5. Quais ameaças e oportunidades do ambiente externo?
6. No ambiente externo, como o cenário atual e futuro afeta os objetivos?
7. Qual a relação do processo com os objetivos estratégicos da Universidade?
8. Quais resultados as partes interessadas esperam do processo/Universidade?
9. O contexto levantado está dentro do apetite a risco da Universidade?

ANEXO II – FORMULÁRIO DE IDENTIFICAÇÃO DE RISCOS

- **UNIDADE**:
- **SERVIDOR**:
- **PROCESSO DE TRABALHO**:
- **OBJETIVO DO PROCESSO DE TRABALHO:**
- **PROPRIETÁRIO DO PROCESSO**:
- **OBJETIVO ESTRATÉGICO RELACIONADO**:
- **DATA DA ANÁLISE**:

ID	EVENTO DE RISCO	CAUSA	CONSEQUÊNCIA	CATEGORIA DO RISCO
R1		*fonte + vulnerabilidade*		
R2		*fonte + vulnerabilidade*		
R3		*fonte + vulnerabilidade*		

APETITE A RISCO DO PROCESSO			
[ ] 🟢 Baixo	[ ] 🟡 Médio	[ ] 🟠 Alto	[ ] 🔴 Extremo

PERGUNTAS DIRECIONADORAS

Para auxiliar na identificação dos riscos, fazer as seguintes perguntas:

1. O que pode atrapalhar o alcance do objetivo do meu processo de trabalho?
2. Quais eventos podem **evitar**, **atrasar**, **prejudicar** ou **impedir** o atingimento do objetivo do processo de trabalho?
3. O evento de risco pode comprometer claramente o objetivo do processo?
4. Qual é a fonte de cada risco?
5. Quais são os motivos (causas) que podem promover a ocorrência do risco?
6. Qual seria o(s) efeito(s) nos objetivos do processo?
7. Qual a categoria do risco?
    a. Operacional
    b. Conformidade
    c. Financeiros/orçamentários
    d. Imagem
    e. Político
    f. Ambiental
    g. Demais riscos

ANEXO III – FORMULÁRIO DE AVALIAÇÃO DE RISCOS

- **UNIDADE**:
- **SERVIDOR**:
- **PROCESSO DE TRABALHO**:
- **OBJETIVO DO PROCESSO DE TRABALHO:**
- **PROPRIETÁRIO DO PROCESSO**:
- **OBJETIVO ESTRATÉGICO RELACIONADO**:
- **DATA DA ANÁLISE**:

ID	EVENTO DE RISCO	AVALIAÇÃO RISCO INERENTE			CONTROLES EXISTENTES			RISCO RESIDUAL	NÍVEL DO RISCO
		PROBABILIDADE	IMPACTO	NÍVEL R.I	DESCRIÇÃO	TIPO DE CONTROLE	NÍVEL DE CONFIANÇA		
R1									
R2									
R3									
R4									

- O cálculo da probabilidade e do impacto deve ser feito considerando as escalas de probabilidade e impacto que constam nos tópicos 5.5.2.3 e 5.5.2.4
- O resultado do risco residual é encontrado multiplicando-se o Nível de Risco Inerente pelo Nível de Confiança do Controle, conforme tabela 5.5.2.6.
- Existindo mais de um controle, deve-se calcular o risco residual de cada um e submetê-los a média aritmética simples.
- Tipos de controle: preventivo, corretivo e detectivo.

PERGUNTAS DIRECIONADORAS

No cálculo da probabilidade e do impacto do evento de risco, assim como na avaliação dos controles existentes, fazer as seguintes perguntas:

1. Qual a chance de o evento ocorrer?
2. Esse evento de risco já ocorreu antes?
3. O contexto de atuação do setor favorece o risco?
4. É frequente a ocorrência deste evento de risco?
5. Qual o impacto/efeito caso esse risco ocorra?
6. O nível de risco é aceitável (apetite a risco)?
7. Existem medidas para controlar esse risco?
8. As medidas existentes para controlar esse risco são eficientes?

ANEXO IV – FORMULÁRIO DE TRATAMENTO DE RISCOS

- **UNIDADE:**
- **SERVIDOR**:
- **PROCESSO DE TRABALHO**:
- **OBJETIVO DO PROCESSO DE TRABALHO:**
- **PROPRIETÁRIO DO PROCESSO**:
- **OBJETIVO ESTRATÉGICO RELACIONADO**:
- **DATA DA ANÁLISE**:

PLANO DE AÇÃO	
Evento de Risco: *Descrição do evento de risco*	**Nível do Risco (Prioridade):** *Baixo, Médio, Alto e Extremo*
Resposta ao Risco: *Aceitar, mitigar, evitar e compartilhar*	**Tipo de controle proposto:** *Preventivo e/ou Corretivo*
Iniciativa (o quê): *Descrever as ações/medidas que serão adotadas para administrar o risco em questão*	
Objetivo (Por que): *Adotar novo controle ou melhorar controle existente?*	
Responsável (Quem): *Servidor(es) responsável pela implementação e controle*	
Como será implementado (Como): *Qual será a estratégia para tratar o risco?*	
Onde? Local onde será feita a ação	
Data de início (Quando): *DD/MM/AAAA*	**Data de término (Quando):** *DD/MM/AAAA*
Custo Previsto (Quanto): *Favorável. Desfavorável*	
Status:	
Monitoramento:	

- O nível do risco e a resposta associada considera a tabela que consta no tópico 5.5.3.3.
- O tipo de controle é preventivo (plano de mitigação) ou corretivo (plano de contingência).
- A iniciativa corresponde a estratégia/ação de tratamento do risco.
- ”Objetivo” se refere a melhorar o controle existente, adotar novo controle ou até mesmo eliminar controle existente.
- ”Como será implementado” informa se por meio de projeto, melhoria no sistema, criação de norma, plano de contingência etc.

- **Status**:

⚫ Não iniciado 🟡 Em andamento

🟢 Concluído 🔴 Atraso

ANEXO V – FORMULÁRIO DE MONITORAMENTO E ANALÍSE CRÍTICA

- **UNIDADE**:
- **SERVIDOR**:
- **PROCESSO DE TRABALHO**:
- **OBJETIVO DO PROCESSO DE TRABALHO:**
- **PROPRIETÁRIO DO PROCESSO**:
- **OBJETIVO ESTRATÉGICO RELACIONADO**:
- **ANALISADO POR**: **DATA DA ANÁLISE**:

MONITORAMENTO E REVISÃO DA GESTÃO DE RISCO	
Responsável: *Servidor que realizará o monitoramento e revisão do risco*	**Frequência**: *Por evento, Mensal, Semestral, Anual*
Houve mudança no processo? *O processo de trabalho foi alterado, com introdução ou retirada de atividades?*	**Novos riscos identificados?** *Sim ou Não*
Novos riscos ou riscos materializados: **R1:**	**Categoria dos novos riscos:** **R1:**
R2:	**R2:**
R3:	**R3:**
Ações corretivas (controles): *Quais ações serão/foram propostas após o monitoramento e revisão do risco.*	***Responsável***: *Servidor(es) encarregados de implementar as melhorias cabíveis*
Lições aprendidas: *Análise crítica da gestão do risco, controles adotados, ferramentas utilizadas, e oportunidades de melhoria.*	
É necessária comunicação com outros setores? Por quê? *É necessário comunicar ou consultar outros setores em função do monitoramento e análise realizada? A melhoria ou ações corretivas envolve outros setores ou servidores?*	
Observações: Comentar detalhadamente as questões: [1] evento de risco [2] quais causas levaram ao risco? [3] quais consequências do risco? [4] os controles adotados pelo setor foram eficientes/funcionais? [5] como foi identificado o risco? [6] quais envolvidos? [7] o risco ocorreu conforme mapeado anteriormente? O que ocorreu? Por que ocorreu? Quando ocorreu? Onde ocorreu? Quanto se perdeu?	

ANEXO VI – FORMULÁRIO DE COMUNICAÇÃO E CONSULTA

- **UNIDADE**:
- **SERVIDOR**:
- **PROCESSO DE TRABALHO**:
- **OBJETIVO DO PROCESSO DE TRABALHO**:
- **PROPRIETÁRIO DO PROCESSO**:
- **OBJETIVO ESTRATÉGICO RELACIONADO**:

COMUNICAÇÃO E CONSULTA				
Interessados	Finalidade	Canal de comunicação	Data da comunicação	Frequência

COMUNICAÇÃO E CONSULTA	
COMUNICAR ALTERAÇÃO DO RISCO? *Sim ou Não*	**DESCRIÇÃO DA ALTERAÇÃO DO RISCO** *Alterações na probabilidade, impacto, causas ou consequências associadas ao risco*
COMUNICAR NOVO RISCO? *Sim ou Não*	**DESCRIÇÃO DO NOVO RISCO** *Novos eventos de risco que surgiram após o mapeamento inicial*
COMUNICAR ALTERAÇÃO DO CONTEXTO? *Sim ou Não*	**DESCRIÇÃO DA ALTERAÇÃO DO CONTEXTO** *Mudanças nas variáveis do contexto interno ou externo que afeta diretamente o processo*
COMUNICAR PLANO DE TRATAMENTO? *Sim ou Não*	**DESCRIÇÃO SOBRE O PLANO DE TRATAMENTO** *Alterações no plano de tratamento ou controles implementados, comunicar o status do plano*
CONSULTAR ORIENTAÇÃO TÉCNICA *Sim ou Não*	**DESCRIÇÃO DA CONSULTA** *Consultar sobre dúvidas, orientações técnicas, metodologia ou outros questionamentos.*
OUTROS (COMUNICAR E CONSULTAR)	**DESCRIÇÃO**

- Finalidade: informar ou consultar.
- Método de comunicação: e-mail, memorando, treinamento, reunião.

- Finalidade
- Frequência: Esporádica, semanal, mensal, trimestral, anual.

ANEXO VII – FORMULÁRIO DE ANÁLISE DA MATURIDADE DA GESTÃO DE RISCOS

Princípios	Item
Alinhamento da gestão de riscos da sua instituição quanto aos seus objetivos estratégicos	Os objetivos da organização ou das atividades em análise foram claramente documentados antes da identificação de riscos?
	A análise de riscos foi conduzida levando em consideração os objetivos da organização e os objetivos da atividade?
	Os objetivos da organização são revisados quando novos riscos são identificados?
	As mudanças nos objetivos são consideradas e refletidas em mudanças da política e da estratégia de riscos?
Adequação da gestão de riscos ao contexto da instituição	Foram conduzidas análises externas ao ambiente da organização, projetos, programa ou operação (ex.: utilizando PESTEL, análise de *stakeholder*, técnica de brainstorming, planejamento de cenários, SWOT)?
	Utiliza-se um processo claramente definido para monitoramento e reavaliação do contexto de risco?
	Utiliza-se uma definição preliminar de quem (departamento/unidade) será o dono de certas categorias de risco num primeiro momento?
	Utiliza-se uma política de gerenciamento de riscos que descreve explicitamente como o risco intervém no contexto organizacional (abrangente, pertinente, viável, seguida)?
Envolvimento das partes interessadas da sua instituição na gestão de riscos	No processo de identificação de risco, são considerados a percepção das partes interessadas, as suas atitudes e os comportamentos?
	A aceitação dos níveis de riscos é debatida ou negociada com as partes interessadas de forma apropriada?
	Utiliza-se atualmente algum mecanismo de fundo de reserva (financeiro) para os níveis de risco acordados?
	A organização estabelece formalmente um registro sobre como evitar a atenuação (subavaliação) de riscos de alto impacto/probabilidade, ou exagero (superavaliação) de riscos de baixo impacto/probabilidade?
Existência de um processo de gestão de riscos bem definido	Utilizam-se uma política de gerenciamento de riscos para a organização em questão?
	Utiliza-se ferramentas e técnicas disponíveis e apropriadas para o gerenciamento de riscos?
	Utiliza-se um canal formalizado para atribuir à alta gestão a responsabilidade dos riscos que excederem a tolerância?
	Utiliza-se uma comunicação formal, por parte da alta gestão, para todos os principais envolvidos da instituição sobre as suas responsabilidades de gerenciamento de riscos?
Tomada de decisão baseada em informações resultantes da gestão de riscos	Os indicadores são regularmente examinados por tomadores de decisão para realizar ações corretivas?
	Utiliza-se uma rotina definida para gerar relatórios periódicos sobre como está sendo realizada a gestão de riscos na sua instituição?
	A alta gestão avalia regularmente o mapa de riscos e implicações financeiras na sua instituição, seus programas, seus projetos ou suas unidades operacionais?
	O nível de resposta ao risco é comensurável (proporcional, adequado) com o nível de risco (ex.: riscos altos possuem ações mais bem elaboradas)?
Facilitação para realização de melhorias contínuas	Existe uma pessoa ou time responsável para melhorar o gerenciamento de riscos na sua instituição, seus programas, seus projetos ou suas operações?
	As práticas são revisadas com base em modelos de maturidade para determinar o nível atingido (atual/presente) e os benefícios correspondentes que podem ser esperados (futuro)?
	A efetividade das respostas aos riscos é monitorada e revisada?
	Utiliza-se um formato, uma estrutura e um conteúdo definidos para apresentar ações de revisão quanto ao tratamento de riscos?
Criação de uma cultura colaborativa quanto à gestão de riscos	A boa gerência de riscos é estimulada pela alta gestão e reconhecida com algum tipo de estímulo/recompensa?
	Utiliza-se um processo de orientação, indução e treinamento sobre gestão de riscos para seus colaboradores, incluindo a alta gestão?
	Boas práticas de gestão de riscos são compartilhadas na instituição com regularidade?
	A alta gestão incentiva um clima de confiança para que os riscos possam ser abertamente discutidos e compartilhados sem temor?
Obtenção de valores mensuráveis associados à gestão de riscos	Utilizam-se medições associadas ao desempenho de gerenciamento de riscos?
	Utiliza-se uma análise de tendências elaborada a partir da gestão de riscos?
	Há evidências de gerenciamento utilizando os dados da análise de tendência para direcionar melhorias futuras?
	A instituição pode demonstrar o retorno de investimento obtido com o desenvolvimento da gestão de riscos?

Esta seção possui perguntas abertas sobre as metodologias de gestão de riscos adotadas e uma escala de 1 (Mais baixa) a 5 (Mais alta) contendo a frequência com que a mão de obra externa é contratada.

Pergunta	Tipo de resposta
Indique quais são as metodologias, as técnicas ou os artefatos de gestão de riscos utilizados pela sua instituição.	Resposta aberta
Com que frequência auditores externos e/ou consultores externos contribuem para gerenciar os riscos da sua instituição?	Escala de 1 a 5

Questões sobre a organização e os colaboradores

Esta seção contém perguntas referentes à sua instituição e aos seus colaboradores.

Afirmativa/ Questão	Item	Tipo de resposta
Indique o seu grau de concordância com as sentenças a seguir:	A missão, a visão e os valores da minha instituição são formulados de maneira clara, sem ambiguidade.	Discordo totalmente; Discordo parcialmente; Nem concordo nem discordo; Concordo parcialmente; Concordo totalmente; N/A/Não desejo responder
	A missão, a visão e os valores da minha instituição são formalizados e comunicados interna e externamente.	
	A soma das metas a serem atingidas reflete os resultados que a organização deseja alcançar.	
	As medidas de desempenho para a minha instituição estão relacionadas com os seus objetivos de forma clara.	
Indique o nível de sua influência nas decisões da alta gestão de sua instituição.	Decisões estratégicas (por exemplo, desenvolvimento de novos produtos ou serviços, desinvestimento de produtos e/ou serviços específicos, estratégias da sua unidade).	Eu possuo toda influência; eu possuo influência parcial; nem eu nem meu superior possuímos influência; meu superior possui influência parcial; meu superior possui toda influência; N/A/Não desejo responder
	Decisões de investimento (por exemplo, mudar para um novo edifício, renovar edifícios, estradas ou outros bens, comprar e implementar novos sistemas de informação).	
	Decisões sobre processos internos (determinação de orçamentos de projetos, definição de prioridades, contratos com fornecedores externos).	
	Decisões relativas às estruturas organizacionais (alteração das estruturas de informação, contratação/demissão de pessoal, compensação, perfis de competências e carreiras profissionais, alteração das estruturas dos comitês).	
Em que grau você concorda com as afirmações seguintes sobre as medidas de desempenho da sua instituição?	Minha instituição possui medidas de desempenho que indicam a quantidade de produtos ou serviços fornecidos.	Discordo totalmente; Discordo parcialmente; Nem concordo nem discordo; Concordo parcialmente; Concordo totalmente; N/A/Não desejo responder
	Minha instituição possui medidas de desempenho que indicam como está a eficiência operacional.	
	Minha instituição possui medidas de desempenho que indicam a satisfação do público atendido.	
	Minha instituição possui medidas de desempenho que indicam a efetividade dos seus resultados.	
Qual é a importância das métricas de desempenho seguintes para a sua remuneração total (ex.: carreira, salário, etc.)?	A importância das "métricas de quantidade" na minha instituição é...	Completamente irrelevante; Pouco relevante; Moderadamente relevante; Importante; Muito importante; N/A/ Não desejo responder
	A importância das "métricas de eficiência" na minha instituição é...	
	A importância das "métricas de satisfação do público atendido" na minha instituição é...	
	A importância das "métricas de resultado" na minha instituição é...	
Compare o desempenho da sua instituição com outras similares (ou compatíveis) nos seguintes itens:	Na quantidade ou montante de trabalho produzido.	Muito abaixo da média; Abaixo da média; Na média; Acima da média; Muito acima da média; N/A/Não desejo responder
	No alcance das metas de produção e de serviço.	
	Na qualidade ou precisão do trabalho produzido.	
	No número de inovações ou ideias novas geradas pelas unidades.	
	Na eficiência da operação.	
	Na reputação no tocante à excelência no trabalho.	
	Na conduta moral dos colaboradores.	

Esta seção contém questões abertas quanto à percepção de riscos dos respondentes.

Pergunta	Tipo de resposta
Justifique a importância da gestão de riscos para a obtenção de resultados pela sua instituição.	Resposta aberta
Na sua percepção, quais são os principais desafios, as dificuldades e as limitações para implantação e realização efetivas da gestão de riscos na instituição?	Resposta aberta

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO 31000. **Gestão de riscos:** princípios e diretrizes, 2009. Disponível em: https://gestravp.files.wordpress.com/2013/06/iso31000-gestc3a3o-de-riscos.pdf

BERMEJO, P. H. de S. et al. **ForRisco**: gerenciamento de riscos em instituições públicas na prática. Brasília: Evobiz, 2018. ISBN 978-85-53102-04-4. Disponível em: http://forrisco.org/Livro_ForRisco.pdf.

BRASIL. Tribunal Superior do Trabalho. **Plano de gestão de riscos da Secretaria do Tribunal Superior do Trabalho**. Brasília: TST, 2015.

BRASIL. Ministério do Planejamento, Orçamento e Gestão e a Controladoria-Geral da União. Instrução Normativa Conjunta nº 1, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo. **Diário Oficial da União**, Brasília, DF, 11 mai. 2016. Seção 1, p. 14. ISSN 1677-7042. Disponível em: https://bit.ly/2BnCKWy.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **Metodologia de gestão de riscos.** Brasília, DF: CGU, 2018.

BRASIL. Tribunal de Contas da União. **Gestão de Riscos: Avaliação da Maturidade**. Brasília, 2018. Disponível em: <https://portal.tcu.gov.br/governanca/governancapublica/gestao-de-riscos/>

Brasil. Tribunal de Contas da União. **10 passos para a boa gestão de riscos**. Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo (Semec), 2018. Disponível em: https://portal.tcu.gov.br/biblioteca-digital/10-passos-para-a-boa-gestao-de-riscos.htm

CFC – Conselho Federal de Contabilidade. Plano de Gestão de Riscos do Conselho Federal de Contabilidade. Disponível em <https://www2.cfc.org.br/sisweb/sre/detalhes_sre.aspx?Codigo=2017/001532&arquivo=Res_1532.doc>

Comitê das Organizações Patrocinadoras da Comissão Treadway - COSO. *Gerenciamento de Riscos Corporativos - Estrutura Integrada*. Disponível em <https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf>

MIRANDA, Rodrigo F. A. **Implementando a gestão de riscos no setor público**. Belo Horizonte: Ed. Fórum, 2017

TCU. Tribunal de Contas da União. **Manual de Gestão de Riscos do TCU.** Brasília,2018. Disponível em: <https://portal.tcu.gov.br/main.jsp?lumPageId=8A8182A24ED12B19014ED646CE5E1FC0&previewItemId=8A81881F64480C8C016466C18121556C&lumItemId=FF8080816364D79801641D8093CE4F64>

UFSB – Universidade Federal do Sul da Bahia. **Plano de Desenvolvimento Institucional** (PID) 2020-2024. Disponível em: <https://ufsb.edu.br/images/Resolu%C3%A7%C3%B5es/2020/PDI_2020-2024_aprovado_Consuni.pdf

UNIFAL-MG - UNIVERSIDADE FEDERAL DE ALFENAS. Plano de Gestão de Riscos da Unifal. Disponível em <**https://www.unifal-mg.edu.br/cgrci/wp-content/uploads/sites/90/2019/10/Plano_Gestao_de_Riscos_Aprovado_18_01_2019-1.pdf.**