TRIBUNAL REGIONAL ELEITORAL DA BAHIA

MANUAL DE GESTÃO DE RISCOS

SALVADOR-BA
OUTUBRO – 2019

EDITORIAL

VERSÃO	**2.1**
DATA DA ELABORAÇÃO	**6/10/2019**

ELABORAÇÃO	**SEGEPRO**
REVISÃO	**COPEG**

APROVAÇÃO	**PRESIDÊNCIA**

SUMÁRIO

ANEXOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

1 APRESENTAÇÃO

Ao longo das últimas décadas, o poder público tem buscado aperfeiçoar a administração de recursos, de forma ágil e eficiente, com aptidão para implementar políticas e programas que entreguem maior valor às partes interessadas, culminando no fortalecimento dos processos de governança institucional, que visam ao estabelecimento de diretrizes e critérios para a racionalização dos recursos humanos, materiais e orçamentários, pautados na eficiência do gasto público e na melhoria contínua dos processos de trabalho.

A busca pelo fortalecimento dos processos de governança institucional, por seu turno, impõe o correto gerenciamento de riscos, que consiste em conjunto de atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos, nos termos do art. 2º, XVI, da Resolução Administrativa TRE-BA nº 16, de 13 de junho de 2018.

O presente Manual de Gestão de Riscos (MGR), concebido como um instrumento de apoio e orientação, detalha os procedimentos e instrumentos necessários para a implementação da gestão de riscos no âmbito do Tribunal Regional Eleitoral da Bahia (TRE-BA), conforme estabelecido na Resolução Administrativa nº 16/2018, publicada no Diário da Justiça Eleitoral (DJE), de 15 de junho de 2018, que institui o Sistema de Gestão de Riscos (SGR) deste Regional Eleitoral.

Nesse sentido, espera-se que este instrumento auxilie os atores da gestão de riscos no exercício da contextualização, identificação, análise, avaliação, tratamento e monitoramento dos riscos sob suas alçadas, simplificando e padronizando a metodologia, no âmbito do TRE-BA.

2 CONCEITOS BÁSICOS

Com o intuito de facilitar a compreensão do conteúdo abordado neste Manual, passa-se a apresentar conceitos básicos relevantes no contexto da gestão de riscos.

GOVERNANÇA

Compreende essencialmente os mecanismos de liderança, estratégia e controle, postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas e à prestação de serviços de interesse da sociedade.

GESTÃO

Conjunto de atividades de planejamento, desenvolvimento, execução e acompanhamento de atividades em consonância com a direção definida pela governança a fim de atingir os objetivos corporativos.

RISCO

Qualquer evento, em potencial, que possa dificultar ou impedir o alcance de objetivos, mensurado em termos de probabilidade e impacto. É o efeito da incerteza nos objetivos de uma organização.

GESTÃO DE RISCOS

Atividades coordenadas voltadas à identificação, análise, avaliação, tratamento e monitoramento de riscos, numa perspectiva de direcionamento e controle, no que tange aos riscos inerentes aos processos de trabalho organizacionais, fornecendo segurança razoável no alcance dos objetivos institucionais.

PROCESSO DE GESTÃO DE RISCOS

Aplicação sistemática de políticas, procedimentos e práticas de gestão em atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica de riscos (ABNT, 2009). Sinônimo de gerenciamento de riscos.

ACCOUNTABILITY PÚBLICA

Conjunto de mecanismos e procedimentos que levam os responsáveis por recursos públicos a prestar contas dos resultados de suas ações, garantindo-se maiores transparência e exposição das políticas públicas. Envolve, além do dever e da responsabilidade de prestar contas, o desejo de fazê-lo de forma voluntária.

Obrigação que têm as pessoas, físicas ou jurídicas, públicas ou privadas, às quais se tenha confiado recursos públicos, de assumir as responsabilidades de ordem fiscal, gerencial e programática que lhes foram conferidas, e de informar a sociedade e a quem lhes delegou essas responsabilidades sobre o cumprimento de objetivos e metas e o desempenho alcançado na gestão dos recursos públicos. É, ainda, obrigação imposta a uma pessoa ou entidade auditada de demonstrar que administrou ou controlou os recursos que lhe foram

confiados em conformidade com os termos segundo os quais eles lhe foram entregues (TCU, 2011).

AS TRÊS LINHAS DE DEFESA

A abordagem das Três linhas de Defesa é uma forma simples e eficaz para melhorar a comunicação e a conscientização sobre os papéis e as responsabilidades essenciais de gestão de riscos e controles.

Por essa abordagem, identificam-se três grupos (ou linhas) envolvidos no gerenciamento eficaz de riscos, com as seguintes funções:

a) 1ª linha de defesa – compõe-se de funções que gerenciam e têm propriedade de riscos, realizando a gestão operacional e os procedimentos rotineiros de riscos e controles internos. Os controles internos são desenvolvidos como sistemas e processos sob sua orientação e responsabilidade. Nesse nível se identificam, avaliam e tratam riscos por meio do desenvolvimento e da implementação de políticas e procedimentos internos que possam oferecer garantia razoável de que as atividades desempenhadas em seu âmbito de atuação estejam de acordo com as metas e objetivos;

b) 2ª linha de defesa – compõe-se de funções que supervisionam riscos, estabelecidas para garantir que a primeira linha funcione como pretendido no que diz respeito à gestão de riscos e controles. Seu papel é coordenar as atividades de gestão de riscos, orientar e monitorar a implementação das práticas de gestão de riscos por parte da gestão operacional;

c) 3ª linha de defesa – compõe-se de funções que fornecem avaliações independentes e objetivas sobre os processos de gestão de riscos, controles internos e governança aos órgãos de governança e à alta administração, tais quais as avaliações realizadas pela auditoria interna.

Figura 1 – Modelo das 3 Linhas de Defesa

3 RESULTADOS ESPERADOS DA GOVERNANÇA COM GESTÃO DE RISCOS

Esta dimensão trata de aspectos relacionados aos efeitos das práticas de gestão de riscos, procurando avaliar em que medida a gestão de riscos tem sido eficaz para a melhoria dos processos de governança e gestão e os resultados da gestão de riscos têm contribuído para os objetivos relacionados à eficiência das operações, à qualidade de bens e serviços, à transparência e à prestação de contas e ao cumprimento de leis e regulamentos (Referencial Básico de Gestão de Riscos, TCU, 2018).

A razão de ser da gestão de riscos é apoiar as organizações na consecução dos resultados planejados. Portanto, todos os objetivos relevantes da organização devem fazer parte do escopo da gestão de riscos, que deverá contribuir para que haja efeitos positivos no alcance de todos eles. Os efeitos produzidos pela gestão de riscos em uma organização se dão em duas esferas: uma de efeitos imediatos e outra de efeitos mediatos. (Referencial Básico de Gestão de Riscos, TCU, 2018).

Constituem-se efeitos imediatos da gestão de riscos (eficácia da gestão de riscos):

- Aprimoramento da qualidade do processo decisório;
- Melhora na coordenação entre as unidades organizacionais;
- Aperfeiçoamento de planos e políticas organizacionais; e
- Otimização da comunicação sobre riscos com partes interessadas e do envolvimento de pessoal com a avaliação e o controle dos riscos.

Já na esfera dos efeitos mediatos, tem-se:

- Melhora do desempenho e previsibilidade dos resultados devido a decisões baseadas em adequado planejamento dos objetivos e no gerenciamento de riscos associados;
- Aumento de valor público entregue à sociedade em troca dos recursos entregues ao poder público para a consecução de seus objetivos (políticas e serviços públicos melhores);
- Reforço no cumprimento das relações de *accountability*, que envolve a transparência e prestação de contas sobre o alcance dos objetivos e resultados planejados e sobre o uso adequado dos recursos públicos, reduzindo as incertezas dos membros da sociedade sobre o que ocorre no interior da administração pública; e
- Aumento da confiança e da segurança da sociedade e dos órgãos de controle em relação às instituições públicas.

4 COMPETÊNCIAS E RESPONSABILIDADES NA GESTÃO DE RISCOS

O processo de gestão de riscos representa o conjunto de atividades contínuas, realizado pelas pessoas em todos os níveis da entidade, desde a definição das estratégias até o nível das atividades operacionais, concebido para identificar riscos que possam afetar a capacidade da organização em atingir os seus objetivos e para apoiar tomadas de decisão e ações que forem necessárias para mantê-los em níveis compatíveis com os limites de exposição a riscos previamente estabelecidos, de maneira a fornecer segurança razoável do cumprimento dos objetivos. Assim, cada pessoa na organização tem uma parcela de responsabilidade na gestão de riscos (Referencial Básico de Gestão de Riscos, TCU, 2018).

Bem por isso, atribuições claras devem ser definidas para que cada grupo de profissionais entenda os limites de suas responsabilidades e como seus cargos se encaixam na estrutura geral de gestão de riscos da organização (IIA, 2013) (Referencial Básico de Gestão de Riscos, TCU, 2018).

Nesse sentido, no âmbito do sistema de gerenciamento de riscos do TRE-BA, o processo de gestão de riscos constitui responsabilidade:

- do Gestor de Riscos;

- do Supervisor de Riscos;

- da Coordenadoria de Planejamento de Estratégia e Gestão (COPEG);

- do Comitê de Segurança da Informação (CSI); e

- do Conselho de Governança.

Nas tabelas abaixo, seguem os integrantes e as atribuições das Três linhas de Defesa adotadas pelo TRE-BA:

Tabela 1 - Linhas de Defesa no Gerenciamento de Riscos no TRE-BA

1ª Linha de Defesa	**2ª Linha de Defesa**	**3ª Linha de Defesa**
Gestores de Risco	**Supervisores de Risco**	
- Assessores - Coordenadores - Chefes de Seção - Chefes de Cartório - Oficiais de Gabinete - Assistentes de Núcleos - Gerentes de projetos - Fiscais de contratos - Titulares de cargos ou funções equivalentes, responsáveis pelos processos de trabalho e iniciativas desenvolvidas no âmbito da Justiça Eleitoral da Bahia	- Presidente do TRE-BA - Vice-Presidente do TRE-BA - Corregedor Regional Eleitoral - Juiz Diretor da Escola Judiciária Eleitoral - Juiz Ouvidor - Juízes Eleitorais da Segunda Instância - Juízes Eleitorais da Primeira Instância - Titular da Diretoria-Geral - Secretários - COPEG	Coordenadoria de Auditoria Interna

Fonte: Resolução Administrativa TRE-BA nº 16/2018.

Tabela 2 – Competências e Responsabilidades no Gerenciamento de Riscos no TRE-BA

AUTORIDADE	COMPETÊNCIAS E RESPONSABILIDADES
Gestores de Risco	▪ Estabelecer as especificidades do contexto para o processo de gestão de riscos, fornecendo subsídios para a elaboração do Plano de Tratamento de Riscos da unidade a que está vinculado, em seus respectivos âmbitos e escopo de atuação; ▪ executar as atividades do processo de gestão de riscos, inclusive daqueles associados à segurança da informação, para os objetos de gestão sob sua responsabilidade; ▪ prover o suporte ao Supervisor de Riscos, na elaboração do Plano de Tratamento de Riscos e dos respectivos relatórios analíticos; ▪ consultar e comunicar as partes interessadas no processo de gestão de riscos, sempre que reputar necessário; ▪ disponibilizar as informações adequadas quanto à gestão dos riscos dos processos sob sua responsabilidade ao Supervisor de Riscos, à COPEG, ao Conselho de Governança e demais partes interessadas; ▪ identificar, analisar e avaliar os riscos dos processos sob sua responsabilidade; ▪ acompanhar a evolução dos níveis de riscos e a efetividade das medidas de controles implementadas nos processos organizacionais sob sua responsabilidade; ▪ informar o Supervisor de Riscos, a COPEG, o Conselho de Governança e demais partes interessadas sobre mudanças significativas nos processos organizacionais sob sua responsabilidade; e ▪ responder às requisições do Supervisor de Riscos, da COPEG, do Conselho de Governança e demais partes interessadas.
Supervisores de Risco	▪ Aprovar e consolidar os Planos de Tratamento de Riscos elaborados pelos gestores de riscos das unidades que lhe forem vinculadas, apresentando o plano consolidado à COPEG e às respectivas revisões anuais, acompanhados de relatórios de ações de gestão de riscos executadas no período; ▪ promover a evolução gradual do Plano de Tratamento de Riscos sob sua supervisão, por meio da identificação, análise, avaliação e resposta a novos riscos, considerando os critérios de priorização e objetos de gestão aprovados pelo Conselho de Governança; ▪ criar, com o apoio da COPEG, e promover a medição de indicador de desempenho relacionado a risco-chave sob sua supervisão, quando assim recomendado pela Secretaria de Planejamento, de Estratégia e de Eleições; ▪ informar à COPEG sobre mudanças significativas nos processos organizacionais sob sua responsabilidade; ▪ responder às requisições da COPEG e do Conselho de Governança; ▪ dirimir dúvida quanto à identificação do Gestor de Riscos referente a processo e iniciativas afetos à sua unidade; ▪ monitorar a evolução dos níveis de riscos e a efetividade das medidas de controles implementadas nos processos organizacionais sob a responsabilidade das unidades que lhes forem vinculadas; e ▪ consultar e comunicar as partes interessadas no processo de gestão de riscos, sempre que reputar necessário.
SPL	▪ Assessorar o Presidente do Tribunal, fornecendo elementos e demais informações necessárias para a tomada de decisão relativa às diretrizes de riscos do TRE-BA, bem como a Alta Administração quanto a riscos estratégicos e riscos-chave; ▪ propor ao Conselho de Governança os critérios e os objetos de gestão de riscos a serem priorizados na evolução dos planos de tratamento das unidades do Tribunal, submetendo a este conselho os relatórios de gestão dos riscos-chave consolidados pela COPEG; ▪ recomendar aos supervisores de riscos a criação e medição de indicador de desempenho para monitoramento de risco-chave sob sua supervisão, quando entender necessário; ▪ propor a formulação de estratégias e diretrizes de gestão de riscos do TRE-BA.

AUTORIDADE	COMPETÊNCIAS E RESPONSABILIDADES
COPEG	▪ Monitorar, sistematicamente, o cumprimento do sistema de gestão de riscos, com vistas a assegurar sua eficácia e o cumprimento dos objetivos, sugerindo melhorias para os procedimentos adotados; ▪ consolidar e submeter à apreciação do Conselho de Governança os relatórios de gestão dos riscos-chave; ▪ acompanhar a efetividade da gestão dos riscos-chave; ▪ orientar os gestores na identificação, análise, avaliação dos riscos, definição de respostas e na elaboração dos planos de gestão de riscos a serem adotados em suas atividades, bem como a criação de indicadores de desempenho, quando for o caso; ▪ consolidar e submeter o Plano de Gestão de Riscos-Chave ao Conselho de Governança para aprovação; ▪ analisar, diligenciar, se necessário, e validar os Planos de Tratamento de Riscos encaminhados pelos Supervisores de Riscos; ▪ propor a metodologia de gerenciamento de riscos do TRE-BA; ▪ propor indicadores de desempenho para acompanhamento da gestão de riscos no Órgão; ▪ apoiar o Secretário de Planejamento de Estratégia e de Eleições nas atribuições relacionadas a riscos; ▪ acompanhar as ações de tratamento e controle dos riscos-chave, a partir dos relatórios consolidados das unidades do Tribunal; e ▪ acompanhar a evolução da maturidade organizacional em gerenciamento de riscos.
Conselho de Governança	▪ Avaliar propostas de limite de exposição a riscos e de melhoria do SGR; ▪ monitorar a situação dos riscos-chave e determinar eventuais ações corretivas; ▪ aprovar o Plano de Gestão de Riscos-Chave; ▪ deliberar sobre indicadores de desempenho para a gestão de riscos no Órgão e os relacionados aos riscos-chave; ▪ garantir o apoio institucional para promover a gestão de riscos, em especial seus recursos, o relacionamento entre as partes interessadas e o desenvolvimento contínuo dos servidores; ▪ emitir e monitorar as recomendações e orientações para o aprimoramento da gestão de riscos; ▪ deliberar sobre gestão de riscos no tocante à segurança da informação; ▪ apreciar relatórios descritivos e analíticos submetidos pela COPEG; ▪ dirimir dúvida suscitada quanto à responsabilidade pela gestão de determinado risco entre unidades representadas no Conselho de Governança; e ▪ praticar outros atos de natureza estratégica e administrativa necessários ao exercício de suas responsabilidades.
Comitê de Segurança da Informação	▪ Apresentar ao Conselho de Governança propostas de diretrizes e políticas para a gestão de riscos relacionados à segurança da informação; ▪ propor aos gestores de riscos processos de trabalho, métodos, técnicas, ferramentas, arquitetura e padrões aplicáveis ao provimento de repostas a riscos relacionados à segurança da informação, observados os princípios e diretrizes estabelecidos; ▪ auxiliar os gestores na identificação, análise, avaliação e tratamento de riscos associados à segurança da informação, promovendo também a identificação e tratamento de vulnerabilidades relacionadas;

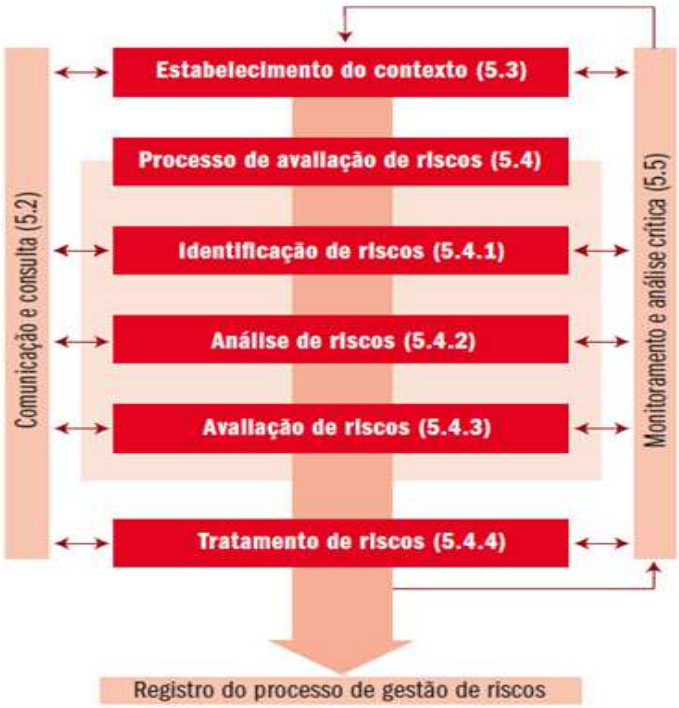
Fonte: Resolução Administrativa TRE-BA nº 16/2018.

5 PROCESSO DE GESTÃO DE RISCOS

Com base nas regras preconizadas pelas Normas ABNT NBR ISO 31000:2009, atualizada em 2018, nos objetivos do Tribunal, bem como nos princípios norteadores de sua gestão de riscos estabelecidos por meio da Resolução Administrativa nº 16/2018, o processo de gestão de

riscos estrutura-se em 5 (cinco) subprocessos principais interdependentes – estabelecimento do contexto; identificação de riscos; análise de riscos; avaliação e priorização de riscos; tratamento de riscos – e 2 (duas) etapas de suporte – comunicação e consulta; e monitoramento e análise crítica, conforme fluxo constante da Figura 2

Figura 2 – Processo de gestão de riscos



Fonte: Referencial Básico de Gestão de Riscos, Tribunal de Contas da União, 2018.

A gestão de riscos é um processo contínuo, que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar riscos capazes de afetar os objetivos, programas, projetos ou processos de trabalho do TRE-BA nos níveis estratégico, tático e operacional.

5.1 ESTABELECIMENTO DO CONTEXTO

O estabelecimento do contexto envolve o entendimento da organização, dos objetivos e do ambiente, no qual os objetivos são perseguidos, com o fim de obter uma visão abrangente dos fatores que podem influenciar a capacidade da organização para atingir seus objetivos, bem como fornecer parâmetros para a definição de como as atividades subsequentes do processo de gestão de riscos serão conduzidas. Contexto é o ambiente no qual a organização busca atingir os seus objetivos. Os objetivos são a essência da definição do contexto, pois a gestão de riscos ocorre no contexto dos objetivos da organização (Referencial Básico de Gestão de Riscos, TCU, 2018).

O estabelecimento do contexto, portanto, é uma pré-condição à identificação de riscos, à análise e avaliação e ao tratamento de risco, compreendendo, portanto, a análise do ambiente interno e externo de inserção da estrutura avaliada, implicando: definição do papel da

estrutura na estratégia organizacional (alinhamento estratégico); análise dos fatores internos e externos facilitadores e dificultadores do alcance dos objetivos, representativos de possíveis fontes de risco; individualização de partes interessadas, interna e externamente, ou seja, dos atores que não estão diretamente envolvidos na execução do processo, mas possuem expectativas em relação a ele; e identificação de partes envolvidas, atores internos responsáveis pela execução do processo, bem como pelo gerenciamento dos riscos e execução dos controles propostos; análise do contexto do processo, ou seja, fluxo de atividades, encadeamento lógico, responsáveis, riscos e controles envolvidos; e, por fim, definição do escopo, abrangência da avaliação de riscos, e critérios de risco, ou seja, parâmetros a serem considerados quando da proposição de estratégias de tratamento de riscos.

Tais aspectos devem ser ponderados tanto em nível geral, para fins de definição, pelo Pleno e pelo Conselho de Governança, de diretrizes, parâmetros e critérios de observância obrigatória em toda a organização, quanto em nível específico, no âmbito de atuação do gestor de risco de determinado processo organizacional. Bem por isso, são considerados os contextos geral e específico, nos seguintes termos:

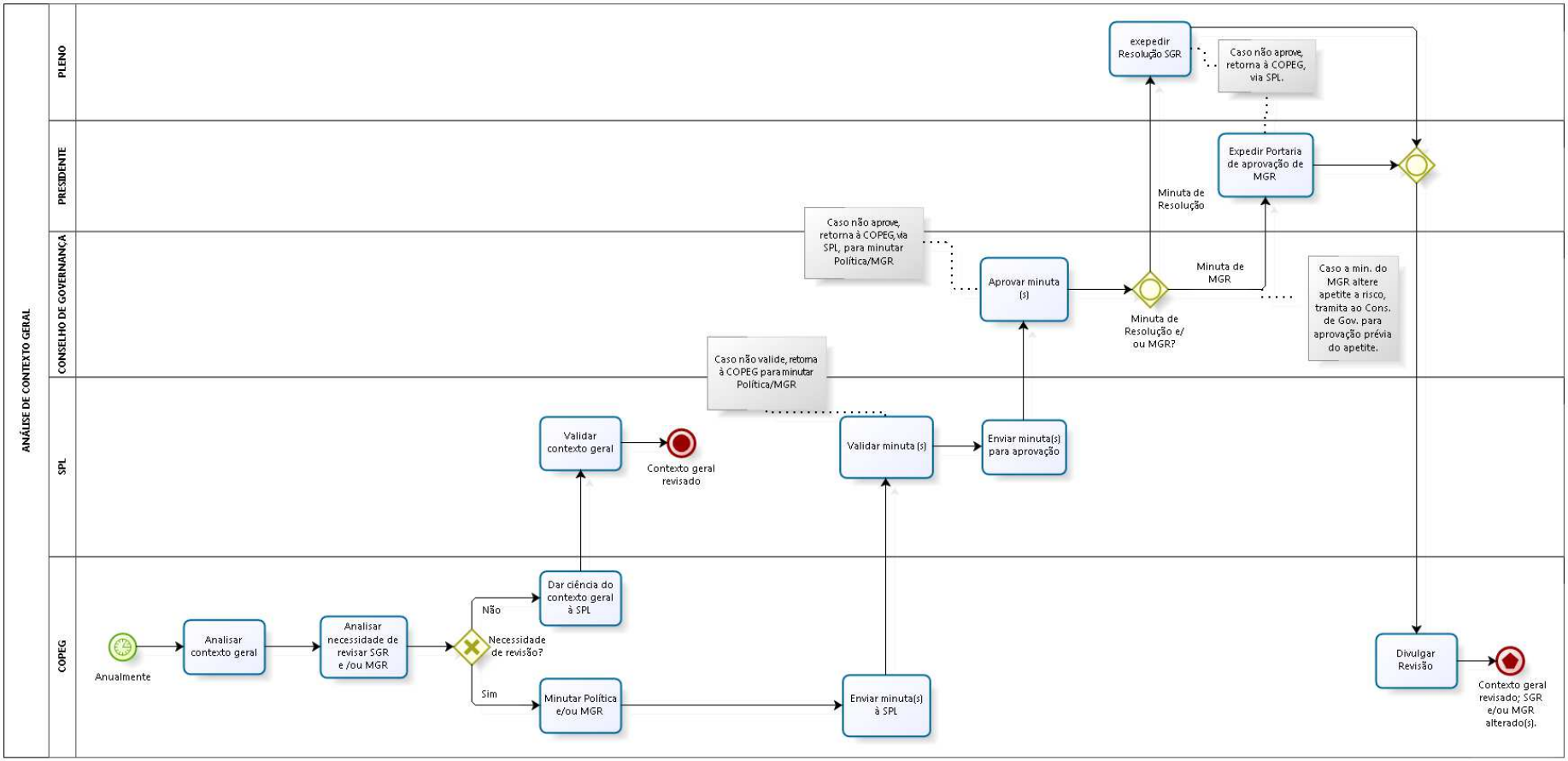
5.1.1 CONTEXTO GERAL

Consiste no estabelecimento dos elementos que envolvem **o sistema de gestão de riscos pelo Pleno**, através de Resolução Administrativa que o discipline e suas respectivas revisões, no que toca à definição dos princípios, dos objetivos, da estrutura, dos papéis e das reponsabilidades, bem como das demais diretrizes que nortearão o processo de gestão de riscos.

Compreende, ainda, a proposta dos referenciais que direcionarão **o processo de gestão de riscos** pela COPEG e SPL, bem como sua aprovação **pelo Conselho de Governança**. Abrange, exemplificadamente, a definição do apetite a risco, dos critérios de riscos, do escopo de aplicação, acompanhamento e monitoramento da gestão de riscos, de ferramentas e/ou modelos adotados no processo de gerenciamento de riscos. Estas definições são formalizadas tanto pelo normativo aprovado pelo Pleno, quanto pelo Manual de Gestão de Riscos (MGR), que é aprovado por Portaria do Presidente do TRE-BA.

Vez que estabelecidas a Política e o MGR do TRE-BA, anualmente deverão ser revisadas as estratégias e diretrizes do sistema e dos procedimentos adotados. Desta revisão anual, podem ser feitos ajustes em alterações do estabelecido nestes documentos, conforme fluxo apresentado a seguir:

Figura 3 - FLUXO – Revisar Diretrizes e Estratégias da Gestão de Riscos



Note-se que, neste momento, não há participação direta do gestor de riscos nem do supervisor de riscos, cingindo-se à atuação da COPEG, da SPL e do Conselho de Governança e do Plenário do TRE-BA, consoante ilustrado nos fluxos acima apresentados.

Para efeito da definição dos aspectos relevantes do sistema de gestão de riscos (SGR), bem como na revisão do manual ao Conselho de Governança, que visa instituir a metodologia e os procedimentos do processo de gestão de riscos, deverão ser considerados os recursos disponíveis (pessoas, tecnologia da informação e comunicação, capacitação, etc.), os fatores internos e externos, facilitadores e dificultadores do alcance dos objetivos e as partes interessadas e envolvidas na consecução dos objetivos da organização e no cumprimento da sua missão institucional, consoante demonstrado nas tabelas abaixo:

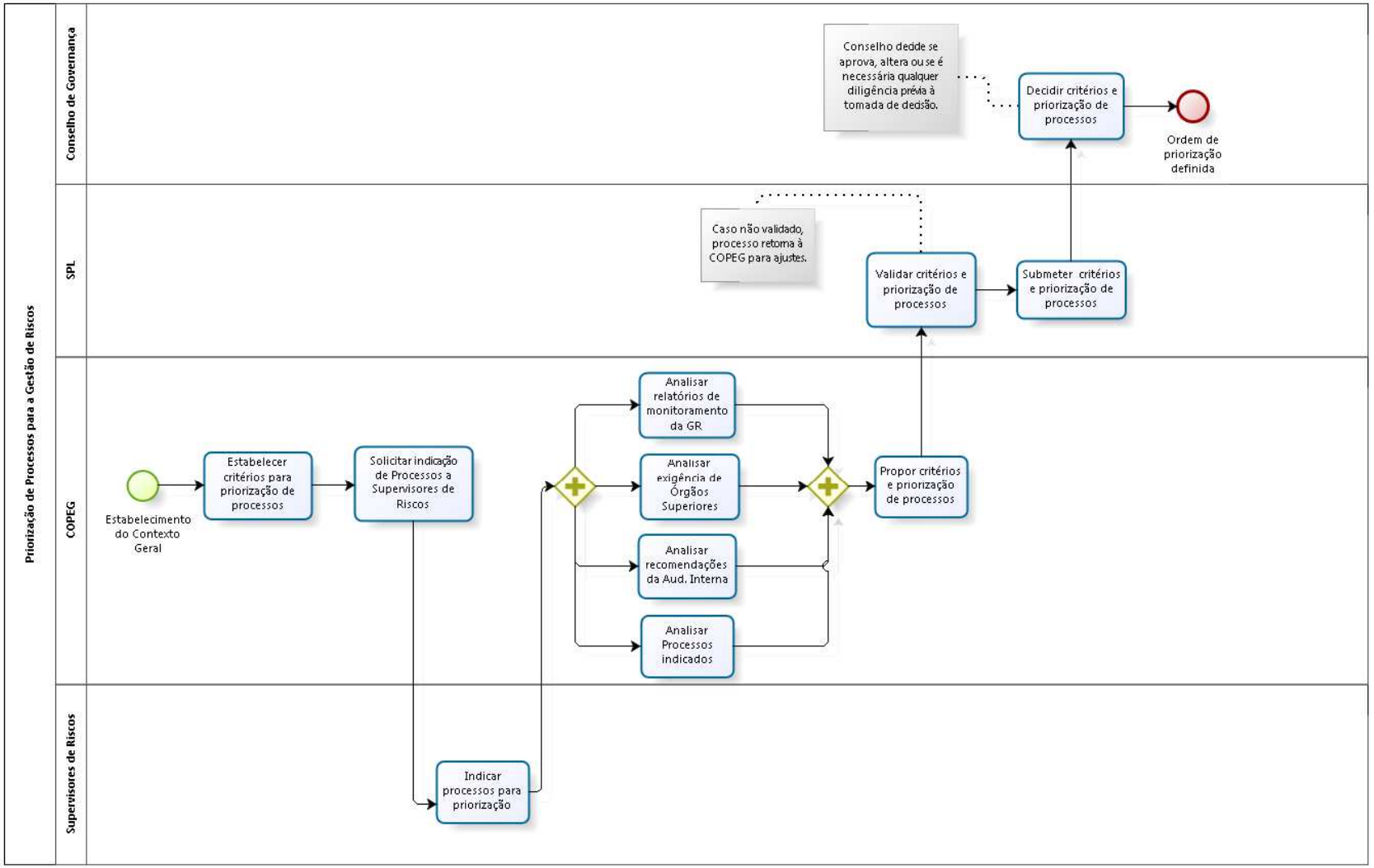
Tabela 3 – Análise SWOT[1] - Contexto Geral

ANÁLISE DO AMBIENTE INTERNO QUE PODE IMPACTAR NA ESTRATÉGIA DO TRE-BA, NA CONSECUÇÃO DOS SEUS OBJETIVOS E NO CUMPRIMENTO DE SUA MISSÃO INSTITUCIONAL	
FORÇAS	**FRAQUEZAS**
ANÁLISE DO AMBIENTE EXTERNO QUE PODE IMPACTAR NA ESTRATÉGIA DO TRE-BA, NA CONSECUÇÃO DOS SEUS OBJETIVOS E NO CUMPRIMENTO DE SUA MISSÃO INSTITUCIONAL	
OPORTUNIDADES	**AMEAÇAS**

Após análise e estabelecimento do contexto geral, será proposta ordem de priorização de processos para integrarem o escopo da consultoria em gestão de riscos no exercício. Os processos priorizados passarão por todas as fases do processo de elaboração dos respectivos planos de tratamento, com as participações das unidades envolvidas, apoiadas pela unidade técnica da COPEG. A seguir ilustra-se o fluxo do processo de **Priorização de Processos para a Gestão de Riscos**:

[1] Matriz SWOT. Ferramenta originária da teoria da Administração, muito disseminada na gestão estratégica. Acrônimo para as palavras inglesas Strengths (Forças), Weaknesses (Fraquezas), Opportunities (Oportunidades) e Threats (Ameaças). Viabiliza análise ambiental ou de cenários e de suas influências no contexto organizacional. No ambiente interno são consideradas as forças e fraquezas (gerenciáveis pela organização) e, no ambiente externo, são identificadas oportunidades e ameaças (alheias à governabilidade da instituição).

Figura 4 - FLUXO – Priorização de Processos para a Gestão de Riscos



Como visto no fluxograma apresentado, constituem insumos para o trabalho desta etapa:

- **relatórios de monitoramento de riscos:** a emissão de relatórios gerenciais acerca da ocorrência de riscos e seus impactos na organização, além da prestação de contas dos gestores de riscos acerca das providências adotadas para tratar os riscos já identificados constituem fonte de informações para o processo de tomada de decisão a respeito da gestão de riscos na instituição e do escopo da consultoria planejada para o exercício;

- **exigências de órgãos superiores:** também são consideradas na definição da ordem de priorização de processos para a gestão de riscos as exigências de órgãos superiores, notadamente o TSE, TCU e CNJ, que constantemente promovem o estabelecimento de boas práticas no âmbito interno. Estes insumos são identificados quando da análise do contexto geral externo ao TRE-BA;

- **indicação de processos pelos Supervisores de Riscos:** em conjunto com a análise dos insumos apresentados, é solicitada aos Supervisores de Riscos a indicação de processos considerados relevantes para o Órgão e que tenham oportunidades de melhoria identificadas, levando em conta, também, os critérios estabelecidos pela COPEG.

- **critérios de relevância estabelecidos:** embora possam sofrer variações de acordo com o contexto vigente, envolvem aspectos como a análise do orçamento associado ao processo, da força de trabalho necessária, do impacto nas metas estratégicas e no grau de satisfação do cliente final, dentre outros.

  A partir da lista de processos indicados pelas áreas interessadas e da análise dos demais fatores citados, é definida proposta de ordem de priorização anual de processos a cumprirem o fluxo da gestão de riscos do TRE-BA.

5.1.2 CONTEXTO ESPECÍFICO

Consiste no estabelecimento das circunstâncias que envolvem o processo organizacional selecionado para a gestão de riscos. Engloba, portanto, as especificidades internas e externas que possam influenciar o processo priorizado. Compreende, exemplificadamente, a análise das partes interessadas, das partes envolvidas, do fluxo do processo organizacional, dos responsáveis, das metodologias e normas específicas e de quaisquer ferramentas, relatórios, modelos, formulários ou sistemas informatizados utilizados no processo organizacional submetido ao gerenciamento de riscos.

Nesta etapa, o processo organizacional e seus objetivos são analisados à luz de seus ambientes interno e externo. Recomenda-se identificar:

- descrição resumida do processo (breve relato sobre o processo, a relação entre os atores envolvidos e os resultados esperados);

- objetivos/Finalidades do objeto de gestão de riscos (apontar quais objetivos são alcançados pelo negócio, atividade ou processo organizacional), podendo ser geral e/ou específicos. Para identificação dos objetivos, pode-se buscar responder à questão "O que deve ser atingido para se concluir que o processo ocorreu com sucesso?";

- unidade responsável pelo processo;

- relação dos objetivos estratégicos associados ao processo;

- periodicidade de execução do processo;

- normativos reguladores do processo (leis, resoluções, instruções normativas, etc);

- sistemas informatizados que dão suporte ao processo;

- partes envolvidas, atores internos responsáveis pela execução do processo, bem como pelo gerenciamento de riscos e execução dos controles propostos;

- partes interessadas, atores internos e externos que, embora não estejam diretamente envolvidos na execução do processo, possuem expectativas em relação a ele;

- informações sobre o contexto interno do processo, considerando as forças e fraquezas que o impactam; e

- informações sobre o contexto externo do processo, considerando cenário atual e futuro, oportunidades e ameaças relacionadas.

As informações mínimas a serem levantadas nesta fase, encontram-se dispostas nas tabelas a seguir, que devem ser preenchidas pelos gestores de riscos:

Tabela 4 – Mapa do Processo (Estabelecimento do Contexto Específico)

ESTABELECIMENTO DO CONTEXTO ESPECÍFICO	
IDENTIFICAÇÃO DO PROCESSO/ATIVIDADE/INICIATIVA:	
OBJETIVO/FINALIDADE:	
PERIODICIDADE DE EXECUÇÃO	
UNIDADE (S) RESPONSÁVEL (IS)	
OBJETIVOS ESTRATÉGICOS DO TRE-BA VINCULADOS AO PROCESSO ORGANIZACIONAL	
NORMATIVOS REGULADORES:	
SISTEMAS INFORMATIZADOS:	
PARTES ENVOLVIDAS:	
PARTES INTERESSADAS:	

FORNECEDORES	ENTRADAS/ INSUMOS	RECURSOS	SAÍDAS/ENTREGAS	CLIENTES

FLUXO DO PROCESSO			
NOME DA ATIVIDADE		DESCRIÇÃO DA ATIVIDADE	RESPONSÁVEL/EXECUTOR
1			
2			

Tabela 5 – Análise SWOT – Contexto Específico

ANÁLISE SWOT[2]	
ANÁLISE DO AMBIENTE INTERNO	
FORÇAS	FRAQUEZAS
ANÁLISE DO AMBIENTE EXTERNO	
OPORTUNIDADES	AMEAÇAS

Levantadas tais informações, é possível desenhar o fluxo do processo organizacional submetido ao gerenciamento de riscos:

- Fluxo (mapa) resumido do processo organizacional (descrição dos fornecedores, entradas/insumos, saídas/entregas e clientes do processo): para se iniciar o processo de identificação dos riscos de qualquer processo ou atividade, é recomendável que se conheça como determinado processo ou atividade é realizado, quais são as etapas, quais as tarefas envolvidas, quem executa, quando executa, de que forma executa. Uma ferramenta bastante utilizada nesse desenho do processo é o fluxograma. Por meio do fluxograma, é possível identificar com mais clareza o encadeamento lógico das atividades ou tarefas que envolvem determinado processo, contribuindo para a análise sistêmica dos processos e dos resultados que cada processo deve entregar.

5.2 IDENTIFICAÇÃO DE RISCOS

Considerando o resultado da etapa de Estabelecimento do Contexto, o desenho do fluxo do processo organizacional, e a experiência do Gestor de Riscos deve-se construir uma lista abrangente de eventos que podem evitar, atrasar, prejudicar ou impedir o cumprimento dos objetivos do processo organizacional ou das suas etapas críticas.

Nesse sentido, a etapa de identificação de riscos compreende a busca, o reconhecimento e a descrição dos riscos relacionados a um objeto de gestão, envolvendo a identificação de possíveis fontes de risco, eventos, causas, consequências e categorias de risco.

Constituem conceitos relevantes da etapa de identificação de riscos:

Risco – qualquer evento, em potencial, que possa dificultar ou impedir o alcance de objetivos, mensurado em termos de probabilidade e impacto. É o efeito da incerteza nos objetivos de uma organização.

Segundo a NBR ISO 31000-2009 (p.2) "*risco é o efeito da incerteza nos objetivos*".

O Coso2 II conceitua risco como a "*possibilidade de que um evento ocorrerá e afetará negativamente a realização dos objetivos*".

O padrão de gestão de risco australiano-neozelandês AS/NZS 43603 (AUSTRALIA, 1999, p.3) define risco como "*a possibilidade de algo acontecer e ter um impacto nos objetivos e é medido em termos de consequências e probabilidades*".

O Tribunal de Contas da União (BRASIL, 2010b), por sua vez, adota definição semelhante à do padrão australiano-neozelandês AS/NZS 4360, conceituando risco como a "*possibilidade de algo acontecer e ter impacto nos objetivos, sendo medido em termos de consequências e probabilidades*".

Observa-se que todas essas conceituações trazem implícita a noção de que riscos estão sempre relacionados a objetivos. A consequência lógica disso é que para se identificar riscos, avaliar sua magnitude e definir se serão modificados por algum tratamento, primeiro é necessário conhecer quais são os objetivos perseguidos.

Elementos do risco - **causa** (fonte/perigo), explorada por uma vulnerabilidade (inexistência, inadequação, insuficiência), que gera um **evento** (incidente/acidente/omissão), levando a **consequências** (ganho/perda). Os riscos, necessariamente, possuem uma ou mais causas, podendo gerar uma ou mais consequências, diretas ou indiretas, e a materialização do risco é denominada evento de risco.

Fonte de risco – elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco, podendo ser tangível ou intangível. São todos os **sujeitos, objetos ou situações** que têm potencial para originar um evento. Classifica-se em seis categorias: **pessoas, processos, sistemas, infraestrutura, tecnologia ou** ainda **eventos externos à organização**.

Causa – condições que dão origem à possibilidade de um evento acontecer, motivos que podem promover a materialização do risco (fontes/perigos). Composta pela associação de vulnerabilidades (inexistência, inadequação, insuficiência) a fonte de risco (pessoas, processos, sistemas, infraestrutura, tecnologia ou eventos externos), exemplos: pessoas sem capacitação, processos mal concebidos, deficiências ou inexistência de controles internos, instalações inadequadas, obsolescência tecnológica etc;

Figura 5 – Causa

(Fonte: Curso de Governança, Gestão de Riscos e Controle Interno no Setor Público, Caderno de Slides, pg.45, Antonio Alves de Carvalho Neto, Salvador/BA, 22 a 24 de agosto de 2018)

Evento - um ou mais incidentes ou ocorrências, proveniente do ambiente interno ou externo, ou mudança em um conjunto específico de circunstâncias, podendo também consistir em algo não acontecer (incidente/acidente/omissão). É a materialização do risco;

Consequência – resultado de um evento que afeta os objetivos. Um mesmo evento pode levar a uma série de consequências;

Figura 6 – Componentes do Risco

Fonte: Curso de Governança, Gestão de Riscos e Controle Interno no Setor Público, Caderno de Slides, pg.45, Antonio Alves de Carvalho Neto, Salvador/BA, 22 a 24 de agosto de 2018.

São categorias de risco, conforme art. 5º da Res. Adm. nº 16/2018:

- Riscos estratégicos – são os relacionados à tomada de decisão pela Alta Administração, que podem impactar o alcance das metas estratégicas;

- Riscos operacionais – são os relacionados a procedimentos ou processos internos;

- Riscos de conformidade – são os relacionados ao não atendimento à legislação, normas e procedimentos vigentes;

- Riscos de imagem – são os que podem comprometer a imagem da instituição junto à população ou a outros órgãos da Administração Pública; e

- Riscos-chave – são os estratégicos e os que, em função do impacto potencial ao TRE-BA, devem ser conhecidos pela Alta Administração;

- Riscos à integridade – são os relacionados à corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, que possam comprometer os valores e padrões preconizados pela organização e a realização de seus objetivos.

  Nesta fase, o gestor de riscos do processo/atividade/iniciativa submetido (a) ao processo de gestão de riscos deverá identificar os eventos de riscos, causas e consequências potenciais, além da categoria de risco. A finalidade é gerar uma lista abrangente de riscos que possam reduzir, atrasar, prejudicar ou impedir a realização dos objetivos. A identificação deverá ser abrangente, pois um risco não identificado nesta fase poderá não ser incluído nas fases posteriores.

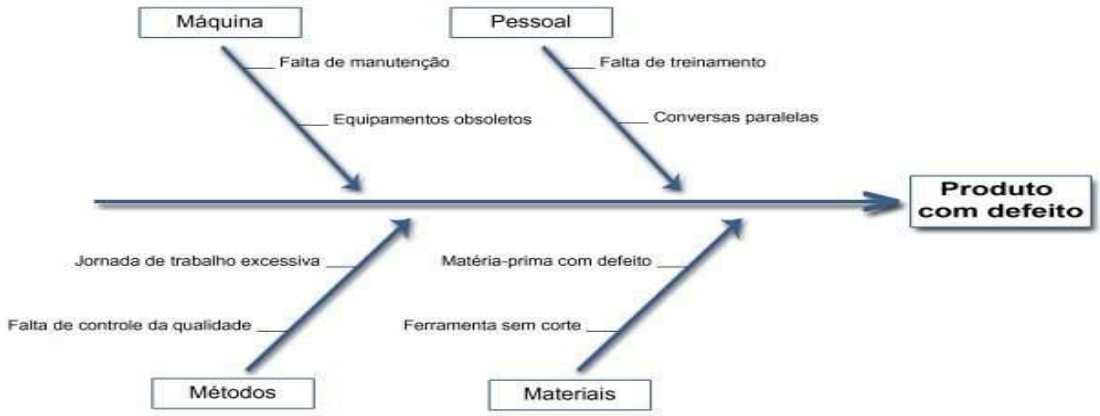
Para esta etapa, podem ser utilizadas técnicas e ferramentas como:

- *Brainstorming* - esta técnica consiste em reunir pessoas conhecedoras de certo ativo ou atividade organizacional e incentivar o fluxo livre de conversação entre elas com o objetivo de identificar possíveis perigos, riscos ou controles associados ao objeto analisado. Consiste, portanto, em técnica de geração de ideias em grupo dividida em duas fases: fase criativa, onde os participantes apresentam o maior número possível de ideias e fase crítica, onde cada participante defende sua ideia com o objetivo de convencer os demais membros do grupo. Na segunda fase são filtradas as melhores ideias, permanecendo somente aquelas aprovadas pelo grupo;

- Entrevistas – formulação prévia de um conjunto de perguntas que servem de guia para o entrevistador e são oportunamente apresentadas às pessoas entrevistadas. Podem ser livres, semiestruturadas ou estruturadas, isto é, com perguntas totalmente pré-definidas, a fim de se garantir que todos os entrevistados abordem as mesmas questões; conduzidas individualmente ou em grupo, com pessoas com experiência no processo ou no projeto, demais envolvidos ou especialistas (que podem ser externos à organização).

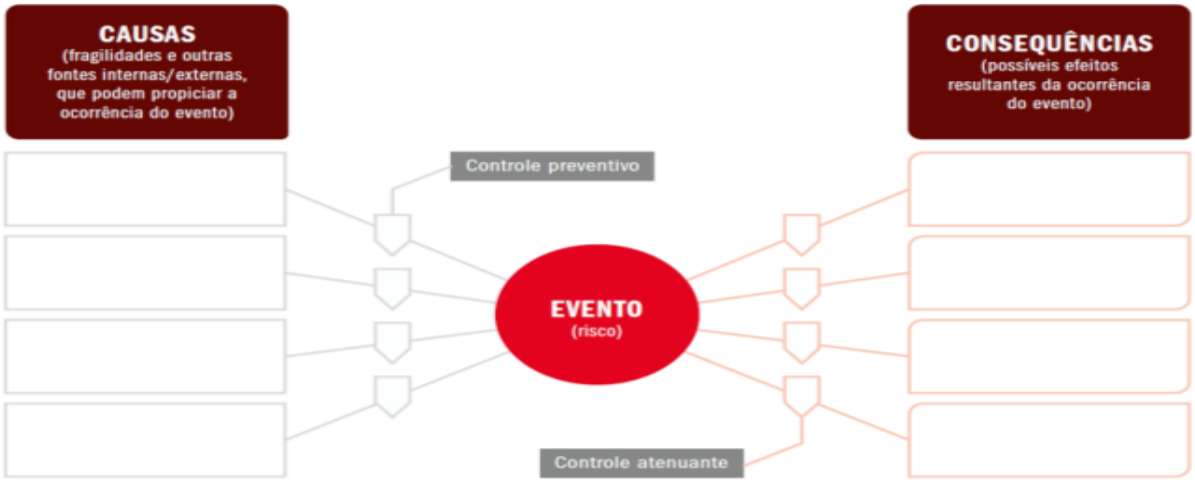
- Diagrama de causa e efeito - também conhecido como diagrama de Ishikawa ou espinha-de-peixe, é útil para a identificação da causa dos riscos. O diagrama é montado organizando o efeito à direita e as causas à esquerda. Para cada efeito existem categorias de causas, como por exemplo: meio ambiente, pessoas, processos, políticas, equipamentos etc.

Figura 7 – Modelo de Diagrama Ishikawa



- Análise *Bow tie* - técnica que busca analisar e descrever os caminhos de um evento de risco, desde suas causas até as consequências, por meio de uma representação pictográfica semelhante a uma gravata borboleta (*bow tie*). O método tem como foco as barreiras entre as causas e o evento de risco e as barreiras entre o evento de risco e suas consequências.

Figura 8 – Modelo de *Bow Tie*



A documentação da etapa de identificação dos riscos geralmente inclui: (a) o escopo do processo, projeto ou atividade coberto pela identificação; (b) os participantes do processo de identificação dos riscos; (c) a abordagem ou o método utilizado para identificação dos riscos e as fontes de informação consultadas; e (d) descrição de cada risco, pelo menos com a fonte de risco, as causas, o evento e as consequências.

O formulário para identificação dos riscos integra o Anexo VI - Matriz de Identificação, Análise, Avaliação, Tratamento e Monitoramento de Riscos. A seguir, os campos que restarão preenchidos ao final desta etapa:

Tabela 6 – Identificação de Riscos

IDENTIFICAÇÃO DE RISCOS							
Processo Organizacional	**Atividade**	**Objetivo/ Finalidade**	**Responsável/ Atividade**	**Evento de Risco**	**Causa**	**Consequência**	**Categoria de Risco**

OBSERVAÇÕES IMPORTANTES SOBRE ESTA ETAPA:

1. Embora o formulário modelo apresentado na tabela 6 especifique "Processo Organizacional" como objeto de gestão de riscos, por ser este, usualmente, o utilizado pela metodologia do Tribunal, o Plano de Tratamento de Riscos poderá ser feito sobre qualquer iniciativa que tenha um objetivo relevante, como planos, projetos, ações ou atividades. Além do grau de importância para a organização/unidade, considera-se o "histórico da ocorrência de problemas" como outro fator preponderante para a priorização da iniciativa na realização da gestão de riscos;

2. Para preenchimento das colunas "Atividade" e "Objetivo/Finalidade" da tabela 6, sugere-se considerar as principais atividades do processo, desconsiderando atividades acessórias, sem relação direta com os objetivos finais da iniciativa como um todo.

É possível, no entanto, dispensar o preenchimento da coluna "Atividades", relacionando a identificação dos riscos diretamente aos objetivos do processo. Neste caso, a coluna "objetivo/finalidade" deverá ser preenchida com base nos objetivos geral e específicos da iniciativa escolhida, e não de suas atividades.

Neste primeiro momento, de amadurecimento da gestão de riscos no TRE-BA, é recomendável a especificação das atividades nesta etapa, podendo os objetivos do processo ser considerados, após, para possível complemento dos riscos já identificados. No entanto, quando a gestão de riscos objetivar exclusivamente a identificação de riscos estratégicos e chave, poderá ser dispensada a consideração das atividades e respectivos objetivos, quando será suprimida a coluna "Atividades", ficando a coluna "Objetivo/Finalidade" para preenchimento dos objetivos geral e específicos da iniciativa (processo, projeto, ação, etc).

DICA PRÁTICA

Da prática da gestão de riscos, observou-se que os objetivos das principais atividades de um processo nada mais são do que os próprios objetivos específicos do processo.

Em um breve resumo, sistematiza-se, a seguir, o roteiro para identificação de riscos:

- ***1º PASSO – Identificar o processo organizacional submetido ao gerenciamento de riscos, bem como os aspectos a ele relacionados (preencher os campos "Processo Organizacional", "Atividade" e "Responsável/Atividade", todos da Tabela 6 – Identificação de Riscos);***

- ***2º PASSO - Identificar as principais funções ou objetivos do processo, ambiente, projeto ou sistema: com base na descrição de processos, ambientes, projetos ou sistemas, o primeiro passo é identificar as principais funções e objetivos que devem***

ser cumpridos pelo objeto que está sendo examinado quanto aos riscos (preencher o campo "Objetivo/Finalidade" da Tabela 6 – Identificação de Riscos);

- ***3º PASSO - Levantar possíveis eventos que podem impedir ou dificultar a execução ou o atingimento dos objetivos do objeto de gest: conhecendo a função e os objetivos de determinado processo, ambiente, projeto ou sistema, torna-se possível identificar o que poderia impactar negativamente a consecução dos objetivos e a inexecução de funções (preencher o campo "Evento de Risco" da Tabela 6 – Identificação de Riscos);***

- ***4º PASSO - Levantar as possíveis causas que levam à ocorrência do evento: após a identificação dos eventos de risco que podem impedir ou dificultar o correto funcionamento de um processo, ambiente, projeto ou sistema, é necessário levantar o que está ocasionando a materialização desses eventos: são as chamadas causas do risco. As causas podem ter diversas origens, tanto internas quanto externas à organização (o que pode ser evidenciado por meio de uma Análise SWOT), podendo advir, exemplificadamente, de falhas humanas, falhas de processos e sistemas, vulnerabilidades sem o devido controle, ação intencional de agentes que exploram tais vulnerabilidades, eventos naturais, dentre outras origens (preencher o campo "Causa" da Tabela 6 – Identificação de Riscos);***

- ***5º PASSO - Levantar as possíveis consequências da ocorrência do evento (levando em consideração os objetivos organizacionais, os objetivos do processos e a conformidade normativa): por fim, a etapa de identificação de riscos deve levantar os potenciais impactos e consequências para os objetivos associados (preencher o campo "Consequência" da Tabela 6 – Identificação de Riscos);***

- ***6º PASSO – Identificar a categoria de risco dentre aquelas categorias previstas no art. 5º, da Resolução Administrativa nº 16/2018, quais sejam, riscos estratégicos, riscos operacionais, riscos de conformidade, riscos de imagem, riscos-chave e riscos à integridade (preencher o campo "Categoria de Risco" da Tabela 6 – Identificação de Riscos).***

5.3 ANÁLISE DE RISCOS

Refere-se ao desenvolvimento da compreensão sobre o risco inerente e à determinação do nível do risco mediante a combinação da probabilidade de sua ocorrência e dos impactos possíveis. Corresponde à etapa de compreender a natureza do risco inerente e determinar o nível de risco, servindo de base para o tratamento dos riscos identificados.

Noutros dizeres, são calculados, nesta etapa, os níveis dos riscos identificados pela equipe técnica designada, a partir de critérios de probabilidade e impacto. Estes (probabilidade e impacto), por seu turno, são estimados mediante escalas quantitativas.

Para melhor compreensão, indica-se a seguir os conceitos envolvidos nesta fase de análise de riscos:

Probabilidade – chance de algo acontecer.

Impacto – resultado de um evento que afeta os objetivos.

Risco Inerente - é o risco próprio, agregado ou inerente à atividade desenvolvida, anterior a qualquer tratamento (risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto). Noutros dizeres, é aquele relativo ao risco do negócio, do processo ou da atividade, independente dos controles adotados.

Nível do risco – medida da importância ou significância do risco, considerando a probabilidade de ocorrência do evento e o seu impacto nos objetivos.

Escala de Probabilidade - define como a probabilidade será medida. A probabilidade está associada às chances de um evento ocorrer. No âmbito do TRE-BA, a probabilidade será avaliada utilizando-se a tabela "Escala de Probabilidade", consoante parâmetros abaixo estabelecidos:

Tabela 7 - Escala de Probabilidade

PROBABILIDADE	DESCRIÇÃO	NÍVEL
Muito Baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias normais indica essa possibilidade. Poderá ocorrer em circunstâncias excepcionais.	1
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade. Não se espera que ocorra.	2
Média	Possível. O evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade. Pode ocorrer em algum momento.	5
Alta	Provável. De forma até esperada o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade. Provavelmente ocorrerá.	8
Muito Alta	Praticamente certa. As circunstâncias indicam claramente a possibilidade do evento ocorrer.	10

Fonte: Referencial Básico de Gestão de Riscos 2018 TCU, com adaptações.

Escala de Impacto - define natureza e tipos de consequências, e como elas serão medidas nas diversas áreas. O impacto está associado às consequências da materialização do evento de risco ocorrido. No âmbito do TRE-BA, o impacto será avaliado utilizando-se a tabela "Escala de Impacto", consoante os parâmetros abaixo estabelecidos (grau de impacto):

Tabela 8 - Escala de Impacto

IMPACTO	DESCRIÇÃO	NÍVEL
Muito baixo	Irrelevante para o alcance do objetivo organizacional e/ou do processo de trabalho associado; não compromete a execução do processo associado; e/ou causa quantidade insignificante de desconformidades com a legislação vigente; e/ou não leva a responsabilização do gestor por ato de improbidade.	1
Baixo	Pouco importante para o alcance do objetivo organizacional e/ou do processo de trabalho associado; não compromete a execução do processo associado; e/ou causa pequena quantidade de desconformidades com a legislação vigente; e/ou não leva a responsabilização do gestor por ato de improbidade.	2
Médio	Importante para o alcance do objetivo organizacional e/ou do processo de trabalho associado; não compromete a execução do processo associado; e/ou causa média quantidade de desconformidades com a legislação vigente; e/ou leva à responsabilização do gestor por ato de improbidade em baixo grau.	5
Alto	Muito importante para o alcance do objetivo organizacional e/ou do processo de trabalho associado; dificulta a execução do processo associado; e/ou causa grande quantidade de desconformidades com a legislação vigente; e/ou leva à responsabilização do gestor por ato de improbidade em médio grau.	8
Muito alto	Essencial para o alcance do objetivo organizacional e/ou do processo de trabalho associado; impede a execução do processo associado; e/ou causa múltiplas desconformidades com a legislação vigente; e/ou leva à responsabilização do gestor por ato de improbidade em alto grau.	10

Fonte: Referencial básico de Gestão de Riscos 2018 TCU, com adaptações.

Matriz 'Impacto X Probabilidade' - define o nível de risco, conforme parâmetros da Tabela 9, a partir dos níveis de probabilidade e impacto.

Tabela 9 - Matriz Impacto x Probabilidade (Nível de Risco)

Nível de Risco		Probabilidade				
		1 Muito Baixa	2 Baixa	5 Média	8 Alta	10 Muito Alta
Impacto	10 Muito Alto	10	20	50	80	100
	8 Alto	8	16	40	64	80
	5 Médio	5	10	25	40	50
	2 Baixo	2	4	10	16	20
	1 Muito Baixo	1	2	5	8	10

Fonte: Referencial básico de Gestão de Riscos 2018 TCU, com adaptações.

Controles Internos - conjunto de regras, métodos, procedimentos, protocolos, rotinas, conferências e trâmite de documentos e informações, entre outros, operacionalizados de forma integrada na organização, destinado a enfrentar os riscos a que ela está exposta e fornecer segurança razoável para a consecução da missão institucional e objetivos organizacionais. São

diversas as classificações dos controles internos, de modo que são abordadas a seguir as mais relevantes:

Quanto à Função:

Essa classificação reflete a função do controle em relação ao risco, isto é, se o controle destina-se a prevenir ou a detectar a materialização de eventos. Dessa forma, os controles classificam-se em:

- **Preventivos** – são concebidos para reduzir a frequência de materialização de eventos de risco, tendendo a agir sobre a probabilidade de ocorrência de um determinado evento, dificultando sua concretização, tais quais: atribuição de autoridade e limites de alçada; procedimentos de autorização e aprovação; segregação de funções; rotatividade de funções; supervisão direta; e controles de acesso a recursos e registros.

- **Detectivos** – detectam a materialização de eventos de riscos, contudo não impedem a sua ocorrência. Alertam sobre a existência de problemas ou desvios do padrão, com o objetivo de provocar a gestão para adotar as ações corretivas pertinentes, tais quais: procedimentos de autorização e aprovação; revisões independentes, verificações e conciliações; avaliação de desempenho operacional; avaliação de operações, processos e atividades; e supervisão direta.

- **Compensatórios -** podem ter função tanto preventiva como detectiva, constituindo-se em controles concebidos para compensar a não adoção de outros controles preventivos ou detectivos, ou para contrabalançar outras falhas na estrutura de controle da organização. A adoção desse tipo de controle normalmente acontece por razões de custo-benefício. É o caso, por exemplo, de se deixar de adotar a segregação de funções ou atividades, por elevar os custos de pessoal, e adotar outras técnicas de controle como análise amostral, inventários cíclicos etc., substituindo, de maneira efetiva, o controle de segregação.

Quanto ao Nível de Abrangência (Controles em nível de entidade e controles em nível de atividades):

CONTROLES EM NÍVEL DE ENTIDADE: são os controles mais abrangentes da organização.

- **Indiretos -** são os controles típicos de “governança corporativa”. Consistem em procedimentos e instrumentos corporativos não ligados diretamente a operações específicas, mas que dão o escopo e evidenciam o tom das ações na organização, estabelecendo critérios e diretrizes de atuação, tais como políticas, regimentos, códigos de conduta, normas e manuais abrangentes, processo de planejamento estratégico, de gestão de riscos, conselhos de administração e fiscal, comitês de auditoria e outros, auditoria interna, ouvidoria (canal de denúncia) etc. Geralmente são preventivos. (Curso Avaliação de Controles

Internos, Aula 01: Bases Conceituais, Instituto Serzedello Corrêa, Tribunal de Contas da União, Junho, 2012, pg.28).

- **Diretos** - controles típicos de "controladoria" – consistem em monitoramentos exercidos pela Alta Administração com o objetivo de identificar eventuais desvios de padrões para, em seguida, aprofundar a investigação de erros ou falhas. Incidem diretamente sobre os processos operacionais da organização, mas não sobre cada transação individual durante o fluxo de operação ou processamento, e sim sobre grupos de transações que já foram total ou parcialmente processadas, tais como análises de variações do tipo "previsto x realizado", revisões de relatórios gerais de desempenho, monitoramento de indicadores etc. Uma característica distintiva desse tipo de controle é o fato de serem, geralmente, detectivos. (Curso Avaliação de Controles Internos, Aula 01: Bases Conceituais, Instituto Serzedello Corrêa, Tribunal de Contas da União, Junho, 2012, pg.29).

CONTROLES EM NÍVEL DE ATIVIDADES: são os controles que incidem direta ou indiretamente sobre atividades, operações, processos ou sistemas específicos.

- **Indiretos ou abrangentes**: definem como fazer. Por exemplo, manuais de processos de trabalho (manual do patrimônio, procedimentos operacionais etc.). Os controles indiretos em nível de atividades – assim como os controles indiretos em nível de entidade – também têm, geralmente, função preventiva. (Curso Avaliação de Controles Internos, Aula 01: Bases Conceituais, Instituto Serzedello Corrêa, Tribunal de Contas da União, Junho, 2012, pg.29).

- **Diretos, de monitoramento ou de registros**: controlam ou evidenciam a execução de atividades durante o fluxo de operação ou processamento. Incidem sobre produtos ou serviços, atividades e tarefas. Exemplos: controles de qualidade na produção (estatístico ou individual), registro de horas despendidas em atividades, registros de produção, conciliações etc. Os controles diretos em nível de processos – assim como os controles diretos em nível de entidade – também têm, em geral, função detectiva. (Curso Avaliação de Controles Internos, Aula 01: Bases Conceituais, Instituto Serzedello Corrêa, Tribunal de Contas da União, Junho, 2012, pg.29).

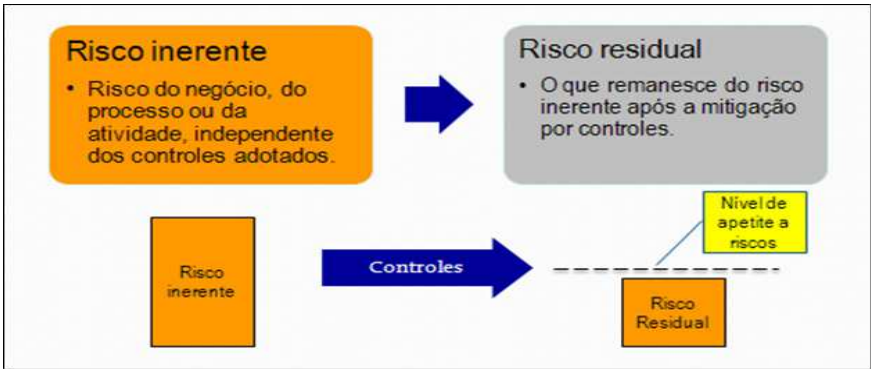
Responsável – aquele a quem se atribui o encargo por determinada atividade, processo, controle ou qualquer outra iniciativa para a consecução dos objetivos institucionais.

Avaliação do controle – é a situação do controle existente tendo como referência a tabela de "Avaliação do Controle". Consiste na definição da eficácia dos controles com base em critérios objetivos estabelecidos para análise dos controles implementados e para cálculo do risco residual.

Risco do Controle – é o risco do controle instituído não tratar o risco satisfatoriamente. Tem como referência a tabela de "Avaliação do Risco do Controle".

Risco Residual – parcela do risco inerente não modificada por tratamento. Risco a que uma organização está exposta após a implementação de ações gerenciais para tratamento do risco. Noutras palavras, o que ainda remanesce após o tratamento por controles. Pode ser chamado de risco retido ou remanescente. Será obtido a partir da multiplicação entre o risco inerente e o risco do controle (Risco Inerente x Risco do Controle).

Figura 9 – Risco Inerente, Risco Residual e Controles



Fonte: Avaliação de Controles Internos, Aula 1: Bases Conceituais, Instituto Serzedello Corrêa, Tribunal de Contas da União.

Ultrapassado esse aspecto introdutório de estabelecimento dos conceitos utilizados nessa fase, passa-se a discorrer sobre as atividades nela envolvidas.

Inicialmente deverão ser fixados os níveis de probabilidade e impacto, levando-se em consideração os critérios indicados nas tabelas 7 e 8.

Em seguida, para definir o risco inerente, os gestores deverão multiplicar a probabilidade da ocorrência do evento de risco pelo seu impacto. Na valoração, poderão associar a probabilidade do evento ocorrer às suas respectivas causas e o impacto às respectivas consequências. Deve-se considerar a probabilidade de ocorrência, bem como o impacto sobre os objetivos levando-se em conta o julgamento dos gestores dos riscos. Por conseguinte, quanto maior a probabilidade e o impacto, maior será o nível do risco inerente.

Para auxiliar nesta atividade, poderá ser preenchido o modelo de tabela abaixo:

Tabela 10 – Análise de Riscos Inerentes

ANÁLISE DOS RISCOS		
Probabilidade	**Impacto**	**Risco Inerente**

Calculado o risco inerente, é possível identificar o seu nível, consoante parâmetros definidos na "**Matriz Impacto x Probabilidade (Nível de Risco)"**, constante da tabela 9.

Passo contínuo, deve-se levantar os controles e seus respectivos responsáveis, analisar os controles identificados e os riscos a eles associados.

A existência de controles já aplicados pressupõe que os níveis de probabilidade e de impacto dos riscos sejam menores do que se não existissem controles. Nesse momento, ainda não se realiza uma análise aprofundada da eficácia dos controles aplicados, apenas constata-se a existência de controles com o intuito de ajudar no processo de avaliação dos riscos. A eficácia e suficiência dos controles será objeto de estudo mais detalhado na fase de Tratamento dos Riscos. Na avaliação dos controles é fundamental a participação do gestor e dos colaboradores responsáveis pela execução do controle para que a avaliação quanto à sua eficácia possa ser o mais fidedigna possível.

Já a informação sobre os responsáveis permitirá o correto direcionamento do processo decisório acerca da estratégia de resposta aos riscos e ao desenvolvimento dos planos de tratamento de riscos. Um aspecto importante é que para se identificar o gestor de um risco, deve-se verificar o evento de risco e a responsabilidade pelo processo que o risco está impactando.

Identificados os controles e respectivos responsáveis, passa-se à avaliação deles, que consiste na etapa de definição da sua eficácia com base em critérios objetivos estabelecidos para análise dos controles implementados e para cálculo do risco residual. Tais critérios objetivos para avaliação dos controles estão definidos na tabela "Avaliação do Risco do Controle"

Tabela 11 - Avaliação do Risco do Controle

NÍVEL DE CONFIANÇA	AVALIAÇÃO DO DESENHO E IMPLEMENTAÇÃO DOS CONTROLES (ATRIBUTOS DO CONTROLE)	RISCO DO CONTROLE
1 – Inexistente Nível de confiança - 0% (0,0)	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	1,00 (muito alto)
2 – Fraco Nível de confiança - 25% (0,25)	Controles têm abordagens *ad hoc*, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo grau de confiança no conhecimento das pessoas, em geral realizado de maneira manual.	0,75 (alto)
3 – Mediano Nível de confiança - 50% (0,50)	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	0,50 (médio)
4 – Satisfatório Nível de confiança - 75% (0,75)	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco consideravelmente.	0,25 (baixo)
5 – Forte Nível de confiança - 95% (0,95)	Controles implementados podem ser considerados a "melhor prática", mitigando adequadamente os aspectos relevantes do risco.	0,05 (muito baixo)

Fonte: Referencial básico de Gestão de Riscos 2018 TCU, com adaptações e alteração da escala.

Note-se que a análise de riscos só se completa quando as ações que a gestão adota para respondê-los são também avaliadas, chegando-se ao nível de risco residual, isto é, o risco que ainda permanece depois de considerado o efeito das respostas adotadas pela gestão para reduzir a probabilidade e o impacto dos riscos, incluindo controles internos e outras ações.

As atividades de controle, também denominadas controles internos, constituem as ações estabelecidas por meio de políticas e procedimentos, desempenhadas em todos os níveis da organização, em vários estágios dentro do processo organizacional e no ambiente tecnológico, que ajudam a garantir o cumprimento das diretrizes determinadas pela administração para mitigar os riscos à realização dos objetivos (COSO, 2013).

Uma forma de avaliar o efeito dos controles internos na mitigação de riscos consiste em estimar a eficácia de cada controle e determinar um nível de confiança (NC), mediante análise dos atributos do desenho e da implementação do controle, conforme delineado na Tabela 11 – Avaliação do Risco do Controle.

Observe-se, a partir da Tabela 11 - Avaliação do Risco do Controle, que ao controle mais bem avaliado atribuiu-se Nível de Confiança (NC) = 95% (0,95). Depreende-se daí que a eficácia do controle interno está sujeita a limitações tanto de implementação como de funcionamento. Assim, não importa quão bem tenham sido desenhados, jamais se pode esperar segurança absoluta. Tais limitações inerentes aos controles podem ser atribuídas a questões como custos *versus* benefícios do controle, erros de julgamento, falhas, conluio, contorno efetuado pela própria administração ou simplesmente erro humano na sua aplicação. Logo, não importa quão efetivo seja o desenho e a implementação de um controle, ele só poderá fornecer uma segurança razoável, nunca absoluta, quanto ao cumprimento dos objetivos para os quais foi concebido.

CUSTO-BENEFÍCIO DO CONTROLE

O custo de se controlar um risco não deve superar os benefícios esperados do controle. A relação custo-benefício é uma limitação ao controle interno justamente porque existem riscos que não são controlados devido ao alto custo que isso implicaria. É bem verdade que essa relação nem sempre pode ser mensurada, cabendo à Administração julgar com base em sua experiência sobre a relação custo-benefício. Isso quer dizer que nem todos os riscos precisam e/ou devem ser controlados. Por exemplo, quando o risco é baixo e o impacto na organização causado pela ocorrência do risco também é baixo, pode-se aceitar o risco e não estabelecer controle interno algum.

No que diz respeito à limitação caracterizada por erro de julgamento, tem-se que a eficácia do controle interno sofre limitações decorrentes das realidades humanas durante a tomada de decisões de negócios, que exige, na maioria das vezes, uma boa parcela de julgamento humano, nem sempre lastreado em informações adequadas e suficientes para suportá-lo. Muitas vezes, decisões tomadas sob pressão de tempo e de outras decorrentes da condução dos negócios podem não refletir os benefícios desejados, necessitando ser mudadas.

Até mesmo controles bem desenhados estão sujeitos a falhas e colapsos. Pessoas podem não entender instruções ou interpretá-las de forma equivocada, ou podem, ainda, cometer erros por fadiga, distração ou falta de cuidado (erros de execução). Erros no desenho do controle (erros de procedimento), por sua vez, podem perpetuar falhas.

Da mesma maneira que as pessoas são responsáveis pelos controles, elas podem valer-se do seu conhecimento e/ou de suas competências para contorná-los com objetivos ilícitos. Responsáveis por um controle podem, individualmente ou em conjunto, agir com vista a burlá-los e a fraudar registros e transações.

Dessa forma, no que toca aos controles internos e suas limitações, pode-se sintetizar as seguintes premissas: controle interno é um meio, e não um fim em si mesmo, integra o processo de gestão (construído “dentro” e não “sobre” os processos de negócio) para fornecer segurança razoável de que objetivos estabelecidos serão alcançados; controle interno auxilia, mas não garante que objetivos serão atingidos e, para ser eficaz, deve ser concebido levando em conta os riscos sobre o alcance desses objetivos; e controle interno é executado por seres humanos, portanto, a sua eficácia deve ser considerada sob a perspectiva da natureza humana.

Para maior detalhamento dos controles internos, auxiliando o responsável pelo gerenciamento de riscos na identificação daqueles já adotados pela gestão, ainda que não de maneira sistematizada e/ou formalizada, indica-se a leitura do Anexo II deste manual.

Uma vez determinado o nível de confiança (NC), pode-se fixar o risco de controle (RC), isto é, a possibilidade de que os controles adotados pela gestão não sejam eficazes para prevenir, detectar e permitir corrigir, em tempo hábil, a ocorrência de eventos que possam afetar adversamente a realização de objetivos. O risco de controle (RC) é definido como complementar ao nível de confiança (NC):

Risco de controle = 1 – Nível de confiança

Fixado o risco do controle, é possível obter o valor do risco residual, a partir do resultado da multiplicação entre o risco inerente e o risco do controle.

Por fim, tem-se que a documentação da etapa de análise de riscos geralmente inclui: (a) abordagem ou o método de análise utilizado, as fontes de informação consultadas e os participantes do processo de análise; (b) as especificações utilizadas para as classificações de probabilidade e impacto dos riscos; (c) a probabilidade de ocorrência de cada evento, a severidade ou magnitude do impacto nos objetivos e sua descrição, bem como considerações quanto à análise desses elementos; (d) a descrição dos controles internos existentes, as considerações quanto à sua eficácia e o risco de controle; e (e) o nível de risco inerente e o residual.

O formulário que orienta a análise dos riscos compõe o Anexo VI - Matriz de Identificação, Análise, Avaliação, Tratamento e Monitoramento de Riscos. Colacionou-se a seguir os campos que restarão preenchidos ao final desta etapa:

Tabela 12 – Análise de Riscos

ANÁLISE							
Probabilidade	**Impacto**	**Risco Inerente**	**Controles Internos**	**Responsável**	**Avaliação do Controle/ Nível de Confiança**	**Risco do Controle**	**Risco Residual**

OBSERVAÇÕES IMPORTANTES SOBRE ESTA ETAPA:

1. Para mensurar probabilidade e impacto, não devem ser consideradas as atividades de controle já realizadas pelo gestor de riscos para mitigar o risco analisado, vez que o risco inerente resultante deste julgamento é o risco próprio da atividade desenvolvida, anterior a qualquer ação gerencial que possa mitigá-lo. Os controles eventualmente utilizados serão considerados após o estabelecimento do nível de risco inerente. Após considerados os controles já praticados sobre o risco inerente, chega-se ao nível de risco residual (o risco que resta após a implementação dos controles).

2. Considerando que pode haver mais de uma causa e consequência para o evento de risco, poderá haver um ou mais controles para mitigá-las. Quando houver mais de um controle, sugere-se que sejam analisados em conjunto, confrontando-os a cada aspecto do risco que pretende atingir. Se, por exemplo, os controles atuarem sobre somente 2 de 3 causas identificadas para o risco, há a possibilidade de melhoria do controle. Caso haja controle sem causa ou consequência correspondente, este pode ser desnecessário, ou a relação de causas e consequências pode estar incompleta.

DICA PRÁTICA:

Como a maioria dos gestores de riscos tem noção do número de ocorrências de materialização de riscos nos processos sob sua responsabilidade, e considerando que estes gestores já trabalham com os controles internos estabelecidos, recomenda-se que o gestor avalie o nível de risco residual resultante de seus julgamentos registrados na planilha de tratamento (análise de probabilidade, impacto e controles), e, se incompatível com a realidade vivenciada no dia a dia do processo (por exemplo, se o risco residual for alto para evento de risco, que, na prática, não se materializa ou não tem impacto relevante), sugere-se rever se as colunas "probabilidade" e "impacto" estão supervalorizadas, ou se a avaliação dos controles foi subdimensionada.

Em um breve resumo, sistematiza-se, a seguir, o roteiro para análise de riscos:

- ***1º PASSO – definir a probabilidade de ocorrência do evento de risco (preencher o campo "probabilidade" da Tabela 10 – Análise de Riscos Inerentes na Tabela 12 – Análise de Riscos, com base nos parâmetros contidos na Tabela 7 – Escala de Probabilidade);***

- ***2º PASSO – definir o impacto das consequências advindas da materialização do evento de risco em análise (preencher o campo "Impacto" na Tabela 10 – Análise de Riscos Inerentes e na Tabela 12 – Análise de Riscos, com base nos parâmetros contidos na Tabela 8 – Escala de Impacto);***

- ***3º PASSO – calcular o risco inerente, multiplicando a probabilidade e o impacto do risco em análise (preencher o campo "Risco Inerente" na Tabela 10 – Análise de Riscos Inerentes e na Tabela 12 – Análise de Riscos com o produto da multiplicação entre a probabilidade de ocorrência do evento e o impacto de suas consequências caso se concretize, conforme se pode visualizar ilustrativamente na Tabela 9 – Matriz ImpactoXProbabilidade – Nível de Risco Inerente);***

- ***4º PASSO – identificar os controles internos preexistentes, bem como o respectivo responsável pela sua execução (preencher os campos "Controles Internos" e "Responsável", ambos da Tabela 12 – Análise de Riscos);***

- ***5º PASSO – indicar o nível de confiança do controle (preencher o campo "Avaliação do Controle/ Nível de Confiança" da Tabela 12 – Análise de Riscos, a partir dos critérios definidos na Coluna 1-Nível de Confiança da Tabela 11 - Avaliação do Risco do Controle);***

- ***6º PASSO - avaliar o risco do controle interno, a partir dos critérios definidos na Tabela 11 – Avaliação do Risco do Controle (preencher o campo "Risco do Controle" da Tabela 12 – Análise de Riscos com o valor atribuído ao risco do controle analisado conforme parâmetros consignados na Tabela 11 – Avaliação do Risco do Controle");***

- ***6º PASSO – calcular o risco residual, multiplicando o risco inerente em análise pelo valor do risco do controle (preencher o campo "Risco Residual" da Tabela 12 – Análise de Riscos com o produto da multiplicação entre risco inerente e risco do controle).***

5.4 AVALIAÇÃO DOS RISCOS

Calculado o valor do risco residual, é possível classificá-lo dentre as seguintes faixas indicadas na tabela 13 (Escala para classificação de níveis de risco):

Tabela 13 – Escala para classificação de níveis de risco

Escala para classificação de níveis de risco			
Risco Muito Baixo/Baixo	Risco Médio	Risco Alto	Risco Muito Alto
1 – 9,99	10-39,99	40-79,99	80-100

Fonte: Referencial básico de Gestão de Riscos 2018 TCU, com adaptações.

A classificação do risco residual corresponde à primeira atividade envolvida nessa fase de avaliação de riscos, servindo as informações produzidas, neste momento, de insumo para a etapa seguinte de tratamento dos riscos.

Essa etapa consiste, portanto, em comparar os resultados da análise de riscos com os critérios de aceitabilidade do risco definidos pelo Conselho de Governança, que não podem ser alterados pelo gestor de risco, visando a apurar se o risco e/ou sua magnitude é aceitável, ou seja, se está dentro do apetite a risco definido para o TRE-BA.

A segunda e última atividade desta fase envolve a comparação do nível de risco residual apurado com os critérios de risco estabelecidos quando o contexto foi considerado, para determinar se o risco e/ou sua magnitude é aceitável ou tolerável ou se algum tratamento é exigido (ABNT, 2009). Noutros dizeres, apura-se se o risco residual está dentro do apetite a risco da organização.

Apetite a Risco, por sua vez, corresponde ao grau de exposição a incertezas que a organização está disposta a aceitar para alcançar seus objetivos. Noutro giro, constitui o nível de risco que uma organização está disposta a aceitar na persecução de seus objetivos.

Neste primeiro estágio de implantação do gerenciamento de riscos no âmbito institucional, o TRE-BA adotou referencial de baixo apetite a riscos, ou seja, o Órgão está disposto a aceitar, mediante monitoramento, baixo nível de riscos, devendo-se, portanto, adotar estratégia de tratamento para os riscos classificados como médio, alto ou muito alto.

Nesse sentido, torna-se imprescindível estabelecer critérios para priorização e tratamento associados aos níveis de risco. A seguir, são trazidas à colação as diretrizes para priorização e tratamento de riscos no âmbito do TRE-BA:

Tabela 14 – Diretrizes para Resposta

Nível de Risco	Descrição	Diretrizes para Resposta
Muito Alto	Nível de risco muito além do apetite a risco da organização.	Requer uma resposta imediata para reduzir, progressivamente, o risco residual ao apetite a risco da organização **(tratar)**.
Alto	Nível de risco além do apetite a risco da organização.	
Médio	Nível de risco acima do apetite a risco da organização.	
Muito Baixo/Baixo	Nível de risco dentro do apetite a risco da organização.	Em regra, nenhuma medida, além das que já forem adotadas, faz-se necessária, impondo-se tão somente seu monitoramento para assegurar que o risco residual se mantenha dentro da margem aceitável. É possível, ainda, que existam oportunidades de ~~maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custo-benefício, como~~ diminuir o nível de controles, desde que não ultrapasse o apetite a risco da organização **(monitorar)**.

Fonte: Referencial básico de Gestão de Riscos 2018 TCU, com adaptações.

Por conseguinte, tem-se que a presente etapa auxilia na tomada de decisão, com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento, especialmente: (a) se um determinado risco precisa de tratamento e a prioridade para isso; (b) se uma determinada atividade deve ser realizada ou descontinuada; e (c) se controles internos devem ser implementados ou, se já existirem, se devem ser modificados, mantidos ou eliminados.

A documentação desta etapa é importante instrumento de *accountability* e geralmente consiste em uma lista dos riscos com suas respectivas classificações e diretrizes para resposta.

Ao final desta etapa, restarão preenchidos os seguintes campos da tabela para a avaliação dos riscos pelos gestores de riscos, que integram o Anexo VI - Matriz de Identificação, Análise, Avaliação, Tratamento e Monitoramento de Riscos deste manual:

Tabela 15 – Avaliação de Riscos

AVALIAÇÃO	
Classificação do Risco	**Diretrizes para resposta**

Em um breve resumo, sistematiza-se, a seguir, o roteiro para avaliação de riscos:

- ***1º PASSO – classificar o valor do risco residual calculado dentre os parâmetros definidos na Tabela 13 – Escala para Classificação de Níveis de Risco (preencher o campo "Classificação do Risco Residual" da Tabela 15 – Avaliação de Riscos, a partir dos parâmetros estabelecidos na Tabela 13 - Escala para classificação de níveis de risco residual);***

- ***2º PASSO – cotejar os níveis de riscos classificados com o apetite a risco da organização para identificar a diretriz para resposta, de modo a indicar o tratamento adequado na fase seguinte (preencher o campo "Diretriz para Resposta" da Tabela 15 – Avaliação de Riscos, de acordo com os parâmetros estabelecidos na Tabela 14 – Diretrizes para Resposta).***

5.5 TRATAMENTO DE RISCOS

O tratamento de riscos compreende a adoção de ações para modificar o nível do risco e a elaboração de planos de tratamento que, uma vez implementados, implicarão em novos controles ou modificação dos existentes. Noutros dizeres, pode-se afirmar que esta etapa será responsável pela seleção e implementação de uma ou mais ações de tratamento para modificar os níveis de riscos.

As opções de tratamento de riscos envolvem as seguintes respostas:

Evitar o risco: ação para evitar totalmente o risco; é a decisão de não iniciar ou de descontinuar a atividade, ou ainda desfazer-se do objeto sujeito ao risco.

Transferir/Compartilhar o risco: compartilhar ou transferir uma parte do risco a terceiros mediante contratação de seguros ou terceirização de atividades nas quais a organização não tem suficiente domínio.

Mitigar/Reduzir o risco: reduzir a probabilidade ou o impacto de ocorrência do risco, ou até mesmo ambos.

Aceitar o risco: é não tomar, **deliberadamente**, nenhuma medida para alterar a probabilidade ou a consequência do risco. Significa aceitar ou tolerar o risco sem que nenhuma ação específica seja tomada, pois ou o nível do risco é considerado baixo ou a capacidade da

organização para tratar o risco é limitada ou o custo é desproporcional ao benefício. Ocorre quando o risco está dentro do nível de tolerância da organização.

Nesse sentido, tem-se que resposta a riscos é o processo de desenvolver e determinar estratégias para gerenciar os riscos. São quatro as categorias de resposta a riscos identificadas na literatura: evitar, reduzir, compartilhar e aceitar. A escolha pela resposta mais adequada dependerá do nível de exposição a riscos previamente estabelecido pela organização em confronto com a avaliação que se fez do risco.

No âmbito do TRE-BA, foram adotados os seguintes padrões de respostas, de acordo com o nível do risco residual:

Tabela 16 – Respostas a Riscos

RISCO ALTO - TRANSFERIR - MITIGAR	**RISCO MUITO ALTO** - EVITAR - TRANSFERIR - MITIGAR
RISCO MUITO BAIXO/BAIXO - ACEITAR	**RISCO MÉDIO** - MITIGAR

Fonte: Referencial básico de Gestão de Riscos 2018 TCU, com adaptações.

Selecionar a opção mais adequada envolve equilibrar, de um lado, os custos e esforços de implementação da medida de mitigação do risco e, de outro, os benefícios decorrentes, levando em consideração que novos riscos podem ser introduzidos pelo tratamento e que existem riscos cujo tratamento preventivo não é economicamente justificável, como riscos de grande consequência negativa, porém com probabilidade muito baixa de acontecer (INTOSAI, 2007; ABNT, 2009).

Ao avaliar os efeitos das diferentes respostas possíveis, a gestão decide a melhor forma de tratar o risco. A resposta ou combinação de respostas selecionada não precisa necessariamente gerar a quantidade mínima de risco residual, mas se gerar um risco residual acima dos limites de exposição estabelecidos, os gestores terão que reconsiderar a opção de resposta ou rever os limites (INTOSAI, 2007).

A título de exemplo indicam-se ações que podem ser adotadas (controles internos), complementarmente a eventuais controles internos preexistentes na gestão, para modificar o nível do risco residual, de modo a compatibilizá-lo com o apetite a risco do TRE-BA: limites de alçada, revisões da Alta Administração, revisão de superiores, normatização interna, manualização e formalização de rotinas, autorizações e aprovações, controles físicos, segregação de funções, capacitação e treinamento, listas de verificação/*checklist*, conciliações, revisão de desempenho operacional, programas de contingência e planos de continuidade dos negócios. Para maior detalhamento acerca de controles internos sugere-se a leitura do Anexo II deste manual.

Impende registrar que, mesmo após o tratamento de determinado risco, haverá risco residual, uma vez que o controle interno fornece asseguração razoável, mas não absoluta na consecução dos objetivos organizacionais, conforme já pontuado.

O Plano de Tratamento de Riscos, por seu turno, é a documentação do tratamento de riscos, que constitui um plano de ação onde são especificados os controles que deverão ser aperfeiçoados ou adicionados, desenvolvidos e implementados, quem será o responsável por eles, e quais são os prazos e recursos requeridos.

Note-se que todas as ações selecionadas devem ter por objetivo reduzir o risco residual para um valor dentro do apetite a risco do TRE-BA, que é baixo (até 9,99), consoante se depreende da Tabela 14 – Diretrizes para Resposta e da Tabela 16 – Respostas a Riscos. Portanto, a meta a ser perseguida não é variável, de modo que o campo "Meta" da tabela 17 – Tratamento de Riscos deve ser fixo, indicando como meta "Risco Baixo/Muito Baixo".

O processo de tratamento é cíclico e inclui: a) avaliação do tratamento já realizado; b) avaliação se os níveis de risco residual são toleráveis; c) se não forem, definição e implementação de tratamento adicional; e d) avaliação da eficácia desse tratamento (ABNT, 2009).

A documentação desta etapa integra o registro de riscos da organização e constitui um plano de tratamento de riscos que deve definir a ordem de prioridade para a implementação de cada ação de tratamento, bem como identificar: (a) os responsáveis pela aprovação e pela implementação do plano; (b) as ações propostas, os recursos requeridos, incluindo arranjos de contingência, e o cronograma; (c) as medidas de desempenho e os requisitos para prestação de informações.

O formulário para auxiliar a fase de tratamento de riscos encontra-se no Anexo VI - Plano de Identificação, Análise, Avaliação, Tratamento e Monitoramento de Riscos, devendo restar preenchidos ao final desta etapa os seguintes campos:

Tabela 17 – Tratamento de Riscos

TRATAMENTO					
Resposta ao Risco	**Ações de Tratamento**	**Responsável**	**Prazo para Implementação**	**Data Inicial**	**Meta**
					"Risco Baixo (até 9,99)"

DICA PRÁTICA:

Na maioria dos casos, prevalece a sabedoria popular de que "prevenir é melhor que remediar", recomendando-se a priorização de controles preventivos, atuantes sobre as causas do evento de risco. Não obstante, controles detectivos e atenuantes, realizados durante e após a materialização de eventos de riscos, podem ser utilizados em complemento aos preventivos, ou isoladamente, quando não for possível a realização de controles prévios ou no caso de serem mais eficientes, diante da análise do custo-benefício dos controles disponíveis.

Em um breve resumo, sistematiza-se, a seguir, o roteiro para o tratamento de riscos:

- ***1º PASSO – identificar a resposta ao nível de risco residual classificado (preencher o campo "Resposta ao Risco" da Tabela 17 – Tratamento de Riscos, a partir dos parâmetros estabelecidos na Tabela 16 – Respostas a Riscos);***

- ***2º PASSO – indicar as ações de tratamento selecionadas para adequar o nível de risco residual classificado para o limite aceitável pelo TRE-BA, isto é, para amoldá-lo ao apetite a risco do Órgão (preencher o campo "Ações de Tratamento" da Tabela 17 – Tratamento de Riscos com controles internos adicionais selecionados pelo gestor de riscos;***

- ***3º PASSO – indicar o responsável pela implementação das ações de tratamento selecionadas (preencher o campo "Responsável" da Tabela 17 – Tratamento de Riscos);***

- ***4º PASSO – indicar o prazo para implementação das ações de tratamento selecionadas (preencher o campo "Prazo para implementação" da Tabela 17 – Tratamento de Riscos);***

- ***5º PASSO – indicar a data para iniciar a implementação da ação de tratamento selecionada (preencher o campo "Data Inicial" da Tabela 17 – Tratamento de Riscos);***

5.6. MONITORAMENTO E ANÁLISE CRÍTICA

Refere-se à contínua verificação, supervisão, observação crítica ou identificação de situação de risco, visando determinar adequação e suficiência dos controles internos associados ao processo de gestão de riscos delineado, de modo a possibilitar ajustes ou melhorias, considerando que o ambiente, os objetivos e o próprio apetite a riscos organizacional podem sofrer alterações ao longo do tempo, inclusive em decorrência do incremento de maturidade dos gestores e executores do plano de tratamento de riscos organizacional.

Ou seja, são finalidades do monitoramento e análise crítica:

- Garantir que os controles sejam eficazes e eficientes no projeto e na operação;

- Obter informações adicionais para melhorar a avaliação dos riscos;

- Analisar os eventos, as mudanças, e aprender com o sucesso ou fracasso do tratamento do risco;

- Detectar mudanças nos contextos externo e interno, incluindo alterações nos critérios de risco e no próprio risco, as quais podem exigir a revisão da forma de tratar os riscos e das prioridades;

- Identificar os riscos emergentes, que poderão surgir após o processo de análise crítica, reiniciando o ciclo do processo de gestão de riscos.

As atividades de monitoramento e análise crítica devem assegurar que o registro de riscos seja mantido atualizado.

A melhoria contínua compreende o aperfeiçoamento ou ajuste de aspectos da gestão de riscos avaliados no monitoramento, constituindo documentação desta etapa o registro das formas de monitoramento da implementação do tratamento dos riscos, representando importante insumo para o aperfeiçoamento dos aspectos afetos ao sistema de gestão de riscos do Órgão, bem como da metodologia do gerenciamento de riscos institucional.

Dentre os instrumentos de monitoramento e análise crítica que podem ser utilizados destacam-se: **acompanhamento de riscos por indicadores** (nível de risco por ativo, processo de trabalho ou ambiente ou grau de redução do nível de risco, por exemplo); **reavaliação de riscos**, considerando possibilidade de alteração de objetivos, de fatores ambientais ou do próprio apetite a risco organizacional; **auditorias baseadas em risco** (avaliação da eficácia do processo de gerenciamento de riscos implementado); r**evisão da política de gestão de riscos e do Manual de Gestão de Riscos**, considerando evolução dos processos internos e da própria maturidade organizacional em gerenciamento de riscos; e **revisão do apetite ou tolerância a riscos** (vide pág 52), tendo em vista eventuais avanços no que tange à maturidade na aplicação de controles.

O formulário para monitoramento e melhoria encontra-se no Anexo VI - Matriz de Identificação, Análise, Avaliação, Tratamento e Monitoramento de Riscos, devendo restar preenchidos, ao final desta etapa, os seguintes campos:

Tabela 18 – Monitoramento de Riscos

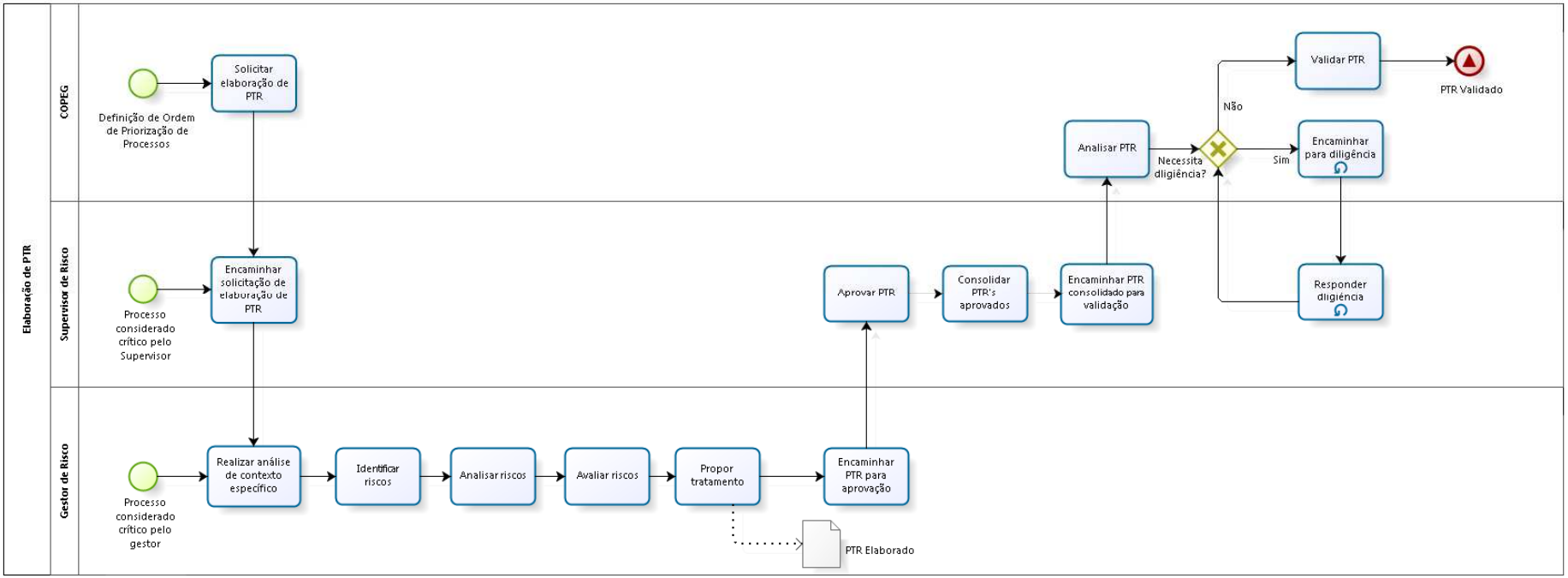
MONITORAMENTO	
Andamento da Ação de Tratamento	**Monitoramento**

Em um breve resumo, sistematiza-se, a seguir, o roteiro para o monitoramento de riscos:

- ***1º PASSO – indicar o estágio da ação de tratamento: a iniciar, em andamento ou concluída (preencher o campo "Andamento da Ação" da Tabela 18 – Monitoramento de Riscos);***

- ***2º PASSO – indicar as formas de monitoramento: indicadores, nesse caso anotar a fórmula de medição, relatórios, etc. (preencher o campo "Monitoramento" da Tabela 18 – Monitoramento de Riscos).***

Figura 10 - Fluxo do Processo Elaboração de Plano de Tratamento de Riscos:



Observa-se que o processo de elaboração do Plano de Tratamento de Riscos (PTR) pode ser provocado pela COPEG ou por iniciativa própria de Supervisores e Gestores de Riscos, caso identifiquem problemas significativos em processos de alta relevância para a organização ou para as respectivas unidades. Uma vez validado o PTR, deve-se iniciar a fase de comunicação às áreas envolvidas e implementação e monitoramento das ações propostas. O plano deve ser revisado sempre que necessário, momento em que riscos, controles e tratamentos estabelecidos são reavaliados, podendo ser identificados novos riscos e formuladas novas ações de tratamento.

6 COMUNICAÇÃO E CONSULTA

As atividades de comunicação e consulta ocupam-se da asseguração da manutenção do fluxo regular e contínuo de informações com as partes interessadas, ocorrendo de forma concomitante ao longo de todas as fases do processo de gestão de riscos, constituindo entrada, inclusive, para a tomada de decisão.

É possível demonstrar graficamente que estas atividades permeiam todo o processo de gerenciamento de riscos, a partir da figura abaixo:

Figura 11 – Ciclo das Atividades de Comunicação e Consulta

Fonte: Conversando sobre riscos, COAUD, 2016.

É importante que durante todas as etapas ou atividades da aplicação do processo de gestão de riscos haja comunicação informativa e consultiva entre a organização e as partes interessadas, internas e externas, para: (a) auxiliar a estabelecer o contexto apropriadamente e assegurar que as visões e percepções das partes interessadas, incluindo necessidades, suposições, conceitos e preocupações sejam identificadas, registradas e levadas em consideração; (b) auxiliar a assegurar que os riscos sejam identificados e analisados adequadamente, reunindo áreas diferentes de especialização; e (c) garantir que todos os envolvidos estejam cientes de seus papéis e responsabilidades, e avalizem e apoiem o tratamento dos riscos. Convêm que seja desenvolvido um Plano de Comunicação pelo Supervisor de Riscos e realizada consulta interna e externa para apoiar essa atividade, seja por meio de documento formal ou de lista de verificação (Referencial Básico de Gestão de Riscos do TCU, 2018).

Revela-se conveniente, portanto, a elaboração de Plano de Comunicação e Consulta, contemplando: público alvo das ações de comunicação (partes interessadas e envolvidas); tipos de informações geradas (relatório, quadro, tabela, inventário, matriz de análise e avaliação, boletim, formulário, agenda, convite, prestação de contas etc.); procedimentos (documentos formais de comunicação interna e externa, correio eletrônico, comunicação instantânea, despacho em processo administrativo, ata de reunião etc.); e periodicidade (frequência), consoante modelo a seguir:

Tabela 19 – Plano de Comunicação e Consulta

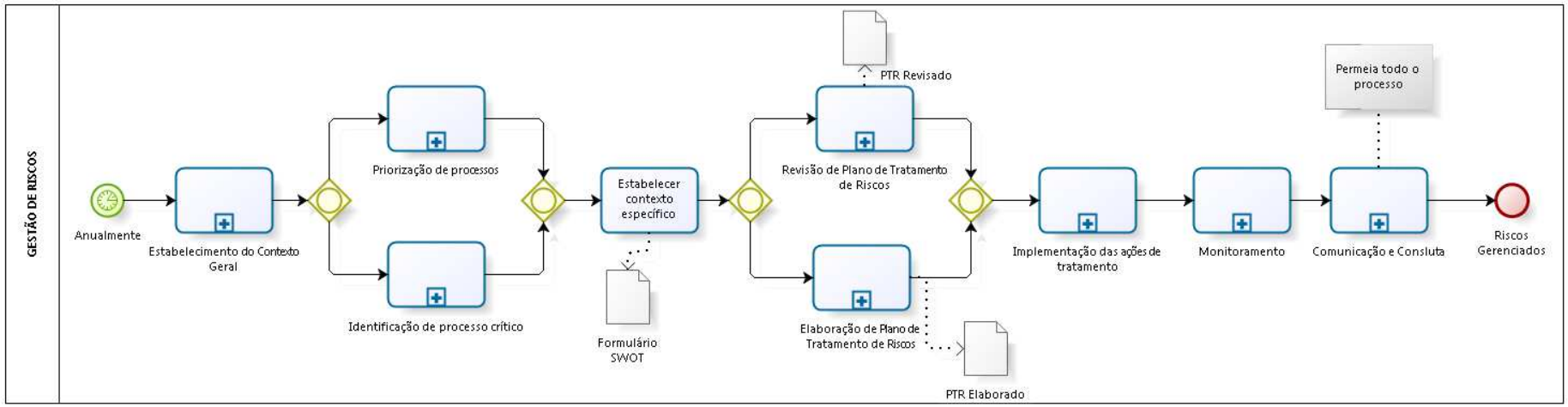
PLANO DE COMUNICAÇÃO E CONSULTA						
PARTES INTERESSADAS E ENVOLVIDAS	**COMUNICADOR**	**OBJETIVO DA COMUNICAÇÃO**	**CONTEÚDO DA MENSAGEM**	**MEIO DE COMUNICAÇÃO**	**PRAZO / DATA/ INÍCIO/**	**FREQUÊNCIA DA COMUNICAÇÃO**

DICA PRÁTICA:

Por ser feita sobre processos que podem percorrer mais de uma função da organização, é comum que o PTR identifique riscos que impactam unidades diversas, ou que ensejem ação atribuída a outrem. Nestes casos, o risco deve ser comunicado aos interessados, e às unidades responsáveis por tratamentos devem ser consultadas sobre a possibilidade e adequação das ações propostas, ajustando-se o plano, se necessário.

Ultimadas todas as fases do ciclo do processo de gestão de riscos, assim se apresenta a visão sistêmica (resumida) de todo o fluxo que se pretende cumprir:

Figura 12 – Visão Sistêmica do Processo de Gestão de Riscos do TRE-BA:



REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Tribunal Regional Eleitoral da Bahia. Resolução Administrativa TRE-BA nº 15, de 13 de junho de 2018. Dispõe sobre o Sistema de Governança e Gestão do Tribunal Regional Eleitoral da Bahia e dá outras providências. Salvador, 2018. Disponível em <http://www.tre-ba.jus.br>.Acesso em: agosto 2018.

_____._____.Resolução Administrativa do TRE-BA nº 16, de 13 de junho de 2018, que institui o Sistema de Gestão de Riscos (SGR) no âmbito do Tribunal Regional Eleitoral da Bahia e dá outras providências. Salvador, 2018. Disponível em <http://www.tre-ba.jus.br>.Acesso em: agosto 2018.

_____._____.Resolução Administrativa TRE-BA nº 17, de 13 de junho de 2018. Institui o Sistema de Governança e Gestão de Tecnologia da Informação e Comunicação (SGTIC) no âmbito do Tribunal Regional Eleitoral da Bahia e dá outras providências. Salvador, 2018. Disponível em <http://www.tre-ba.jus.br>.Acesso em: agosto 2018.

_____.Ministério do Planejamento, Orçamento e Gestão e 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 federal. Brasília, 2016. Disponível em <http://www.cgu.gov.br/sobre/legislacao/arquivos/instrucoes-normativas/in_cgu_mpog_01_2016.pdf>. Acesso em: agosto 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. NBR ISO 31000: Gestão de riscos: Princípios e diretrizes. Rio de Janeiro, 2009.

BRASIL. Tribunal de Contas da União. Referencial básico de Gestão de Riscos/Tribunal de Contas da União. Brasília, 2018.

_____._____. Gestão de Riscos – Avaliação da Maturidade/Tribunal de Contas da União. Brasília, 2018.

_____._____. 10 Passos para a Boa Gestão de Riscos/Tribunal de Contas da União. Brasília, 2018.

_____.Tribunal Regional do Trabalho da 8ª Região. Portaria da Presidência do TRT 8ª Região nº 1068, de 13 de novembro de 2015. Institui o Manual de Gestão de Riscos do Tribunal Regional do Trabalho da 8º Região. Pará, 2015. Disponível em <https://www.trt8.jus.br/governanca/gestao-de-riscos>.Acesso em: agosto 2018.

_____.Tribunal Regional Eleitoral da Bahia. Curso Gestão de Riscos – Princípios e Diretrizes. Antonio Alves de Carvalho Neto. Presencial - Salvador, sala de treinamento do TRE-BA, 22 a 24 de agosto de 2018.

_____._____. Palestra – Conversando sobre a Gestão de Riscos. Fernanda Costa Guimarães. Presencial (slides) – Salvador: Sala de Sessões do Tribunal Regional Eleitoral da Bahia, 2016.

_____.Tribunal de Contas da União. Curso Avaliação de Controles Internos – Aulas 1 e 2 (Apostila) – Brasília: TCU, Instituto Serzedello Corrêa, 2012.

ANEXO I

GLOSSÁRIO

Análise de Riscos – processo de compreender a natureza do risco e determinar o seu nível, fornecendo a base para a avaliação de riscos e para as decisões sobre o respectivo tratamento, incluindo a estimativa de riscos.

Apetite ao Risco – grau de exposição a incertezas que a organização está disposta a aceitar para alcançar seus objetivos. Noutros dizeres, constitui o nível de risco que uma organização está disposta a aceitar na persecução de seus objetivos. Neste primeiro estágio de implantação do gerenciamento de riscos no âmbito institucional, o TRE-BA adotou referencial de baixo apetite ou tolerância riscos, ou seja, o Órgão está disposto a aceitar, mediante monitoramento, baixo nível de riscos, devendo, portanto, adotar estratégia de tratamento para os riscos classificados como médio, alto ou extremo.

Avaliação do controle – é a situação do controle existente tendo como referência a tabela de "Avaliação do Controle". Consiste na definição da eficácia dos controles com base em critérios objetivos estabelecidos para análise dos controles implementados e para cálculo do risco residual.

Categorias de Riscos - as categorias de riscos estão definidas no art. 5º da Resolução Administrativa nº 16/2018 e abrangem riscos estratégicos, operacionais, de conformidade, de imagem e riscos-chave.

Causa – Condições que dão origem à possibilidade de um evento acontecer, motivos que podem promover a ocorrência do risco (fontes/perigos);

Classificação do Risco – Nível de risco residual a que a organização está exposta.

Comunicação e consulta – constitui etapa de suporte ao processo de gestão de riscos que se ocupa da asseguração da manutenção do fluxo regular e contínuo de informações com as partes interessadas, ocorrendo de forma concomitante ao longo de todas as fases do processo de gestão de riscos, constituindo entrada, inclusive, no caso da consulta, para a tomada de decisão.

Consequência – Resultado de um evento que afeta os objetivos.

Contexto específico – estabelecimento das circunstâncias que envolvem o processo organizacional selecionado para a gestão de riscos. Circunscreve-se ao âmbito de atuação do gestor de risco. Compreende, exemplificadamente, a definição das partes interessadas, das partes envolvidas, do fluxo do processo organizacional, dos responsáveis, das metodologias e normas específicas, das ferramentas/relatórios/modelos/formulários/sistemas informatizados envolvidos no processo organizacional submetido ao gerenciamento de riscos.

Contexto externo – ambiente externo no qual a organização busca atingir seus objetivos, podendo incluir o ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, seja internacional, nacional, regional ou local, os fatores chaves e as tendências que tenham impacto sobre os objetivos da organização e as relações com partes interessadas externas e suas percepções e valores.

Contexto geral - estabelecimento dos elementos que envolvem o processo de gestão de riscos. Circunscreve-se à proposta dos referenciais que nortearão o processo de gestão de riscos e a sua aprovação pelo Conselho de Governança. Compreende, exemplificadamente, a definição do apetite a risco, dos critérios de riscos, do escopo de aplicação, acompanhamento e monitoramento da gestão de riscos, de ferramentas e/ou modelos adotados nesse processo de gerenciamento de riscos.

Contexto interno – ambiente interno no qual a organização busca atingir seus objetivos, podendo incluir a governança, estrutura organizacional, funções, responsabilidades, políticas, objetivos e estratégias implementadas para atingi-los, capacidades compreendidas em termos de recursos e conhecimento, sistemas de informação, fluxos de informação e processos de tomada de decisão, relações com partes interessadas internas e suas percepções e valores, cultura da organização, normas, diretrizes e modelos adotados pela organização e forma e extensão das relações contratuais.

Controles Internos – conjunto de regras, métodos, procedimentos, protocolos, rotinas, conferências e trâmite de documentos e informações, entre outros, operacionalizados de forma integrada na organização, destinados a enfrentar os riscos a que ela está exposta e fornecer segurança razoável para a consecução da missão institucional e objetivos organizacionais. Noutros dizeres, é o que se faz para tratar riscos, assegurando, assim, com certa razoabilidade, que objetivos sejam alcançados.

Critérios de risco – termos de referência contra os quais a significância de um risco é avaliada, podendo ser baseados nos objetivos organizacionais, no contexto interno/externo ou derivados de normas, leis, políticas e outros requisitos. Correspondem aos parâmetros que deverão ser considerados quando da proposição de estratégias de tratamento de riscos.

Elementos do risco - causa (fonte/perigo), explorada por uma vulnerabilidade, gerando um evento (incidente/acidente/omissão), levando a consequências (ganho/perda). Assim, os riscos, necessariamente, possuem uma ou mais causas (ações ou omissões de indivíduos, fonte de risco inerente), podendo gerar uma ou mais consequências, diretas ou indiretas (perdas ou ganhos) e a materialização do risco é denominada evento de risco.

Escopo - limite ou abrangência do gerenciamento de riscos em face da estrutura avaliada.

Estabelecimento de contexto – etapa que visa à definição dos parâmetros gerais e específicos, externos e internos a serem levados em consideração ao gerenciar riscos, do escopo e dos critérios de risco para a política de gestão de riscos.

Evento - um ou mais incidentes ou ocorrências, proveniente do ambiente interno ou externo, ou mudança em um conjunto específico de circunstâncias, podendo também consistir em algo não acontecer (incidente/acidente/omissão).

Gerenciamento de riscos à integridade - adoção de controles internos com o objetivo de diminuir o risco de corrupção e fraudes, condutas ilegais e/ou antiéticas, bem como aumentar a capacidade de detecção e remediações das irregularidades que venham a ocorrer, com vistas a fornecer segurança razoável quanto ao cumprimento dos objetivos institucionais.

Gestão - conjunto de atividades de planejamento, desenvolvimento, execução e acompanhamento de atividades em consonância com a direção definida pela governança a fim de atingir os objetivos corporativos.

Gestão de Riscos – atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos. Atividades coordenadas voltadas à identificação, análise, classificação, avaliação e tratamento de riscos, numa perspectiva de direcionamento e controle, no que tange aos riscos inerentes aos processos de trabalho organizacionais, fornecendo segurança razoável no alcance dos objetivos institucionais.

Gestor de Riscos – servidor com autoridade e responsabilidade para gerenciar riscos e com competência para orientar e acompanhar as ações de identificação, avaliação, resposta e monitoramento de risco. Conforme definido no art. 8º da Resolução Administrativa nº 16/2018, são considerados gestores de riscos em seus respectivos âmbitos e escopos de atuação: os Assessores, os Coordenadores, os Chefes de Seção, os Chefes de Cartório, os Oficiais de Gabinete, os Assistentes de Núcleos, os gerentes de projetos e os fiscais de contratos. Ainda, conforme definido no parágrafo único do referido artigo, são também considerados gestores de riscos os titulares de cargos ou funções equivalentes, responsáveis pelos processos de trabalho e iniciativas desenvolvidas no âmbito da Justiça Eleitoral da Bahia.

Governança – compreende essencialmente os mecanismos de liderança, estratégia e controle, postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas e à prestação de serviços de interesse da sociedade.

Impacto – resultado de um evento que afeta os objetivos.

Manual de Gestão de Riscos – conjunto de procedimentos sistematizados que definem uma metodologia de gestão de riscos para a organização, a fim de orientar os gestores na condução dos processos, projetos e atividades.

Monitoramento – verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado. Tem como objetivo avaliar a qualidade da gestão de riscos e dos controles internos da gestão, por meio de atividades gerenciais contínuas e/ou avaliações independentes, buscando assegurar que estes funcionem como previsto e que sejam modificados apropriadamente, de acordo com mudanças nas condições que alterem o nível de exposição a riscos.

Nível do risco – medida da importância ou significância do risco, considerando a probabilidade de ocorrência do evento e o seu impacto nos objetivos.

Objeto de gestão de riscos – qualquer processo de trabalho, atividade, projeto, iniciativa, ação ou plano institucional, assim como os recursos que dão suporte à realização dos objetivos da organização.

Organização estendida – conjunto de interdependências da instituição com outras organizações.

Partes envolvidas – constituem os atores internos responsáveis pela execução do processo, bem como pelo gerenciamento dos riscos e execução dos controles propostos

Partes interessadas – pessoas ou organizações que podem afetar, ser afetadas ou perceberem-se afetadas por uma decisão ou atividade. constituem os atores que não estão diretamente envolvidos na execução do processo, mas possuem expectativas em relação a ele. Exemplificadamente, no âmbito interno, a Presidência e, no âmbito externo, o TSE, o CNJ e o TCU, que guardam expectativas em relação à gestão administrativa do Tribunal, inclusive sob a ótica orçamentária e de resultados.

Perfil de risco – descrição de um conjunto qualquer de riscos que dizem respeito a toda a organização, parte da organização, ou referente ao qual tiver sido definido.

Plano de Gestão de Riscos-Chave – conjunto de ações deliberadas pelo Conselho de Governança, embasado nos objetivos estratégicos e nos planos de tratamento de riscos propostos pelos supervisores de riscos.

Plano de Tratamento de Riscos – conjunto de ações selecionadas pelos gestores de riscos, com indicação de procedimentos, atribuições de responsabilidades e prazos para implementação, com vistas a identificar, avaliar, tratar e monitorar os riscos dos processos institucionais.

Política – instruções claras e mensuráveis de direção e comportamento desejado de forma a condicionar as decisões tomadas no âmbito da instituição.

Política de Gestão de Riscos – declaração das intenções e diretrizes gerais de uma organização relacionada à gestão de riscos.

Probabilidade – chance de algo acontecer.

Processo – aplicação sistemática de políticas, procedimentos, práticas e atividades, visando ao alcance de objetivos ou à entrega de produtos e serviços.

Processo de Avaliação de Riscos – processo global de identificação, análise e avaliação de riscos. Compreende o processo de determinar se o risco e/ou sua magnitude ou grau é aceitável ou tolerável para a organização. Auxilia na decisão sobre o tratamento de riscos, devendo levar em consideração o julgamento dos gestores dos riscos.

Processo de Gestão de Riscos - aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos.

Processo de Trabalho - para as finalidades da metodologia de Gestão de Riscos da Secretaria do TRE-BA, processo de trabalho são os processos, projetos e ações relacionadas às competências e atribuições das unidades do Tribunal.

Responsável – aquele a quem se atribui o encargo por determinada atividade, processo, controle ou qualquer outra iniciativa para a consecução dos objetivos institucionais.

Resposta a risco – corresponde ao desenvolvimento e determinação de estratégias para gerenciar os riscos identificados. São quatro as categorias de resposta a riscos: evitar, reduzir, compartilhar e aceitar, cuja escolha dependerá do nível de exposição a riscos previamente estabelecido pela organização em confronto com a avaliação que se fez do risco.

Risco – efeito da incerteza sobre os objetivos, medido em termos de probabilidade e impacto. Qualquer evento, em potencial, que possa dificultar ou impedir o alcance de objetivos, mensurado em termos de probabilidade e impacto.

Risco à integridade - evento relacionado a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, que possa comprometer os valores e padrões preconizados pela Instituição e a realização de seus objetivos.

Risco do Controle – é o risco do controle instituído não tratar o risco satisfatoriamente. Tem como referência a tabela de "Avaliação do Risco do Controle".

Risco Inerente – é o risco próprio, agregado ou inerente à atividade desenvolvida, anterior a qualquer tratamento.

Risco Residual – parcela do risco inerente não modificada por tratamento. Pode ser chamado de risco retido ou remanescente.

Tratamento de riscos – processo para modificar o risco.

Tolerância a riscos – tolerância a riscos é a variação aceitável quanto à realização de um objetivo específico. É uma derivação tolerável dos objetivos organizacionais (exemplo: projetos devem ser concluídos no prazo e dentro do orçamento estipulado, mas uma variação de até 15% no prazo e de até 10% no custo total é tolerada).

No âmbito do TRE-BA, nesse primeiro momento de institucionalização do gerenciamento de riscos, a tolerância deverá ser fixada para os objetivos estratégicos institucionais, pela COPEG, para aqueles indicadores de desempenho do Planejamento Estratégico 2016-2021 que admitam variação aceitável de desempenho, podendo ser adotada também pelos demais responsáveis pelo gerenciamento de riscos no âmbito institucional.

Violação de integridade - ação ou omissão de um ou mais agentes relacionada à quebra de valores e padrões preconizados pela organização, normalmente associados à corrupção, fraude, irregularidades e desvios éticos e de conduta.

ANEXO II

CONTROLES INTERNOS

Visando auxiliar o responsável pelo gerenciamento de riscos na identificação e avaliação dos controles internos, na fase de análise de riscos, bem como na propositura de controles internos adicionais para reduzir o risco residual ao apetite a risco da Organização, na fase de tratamento de riscos, buscou-se reproduzir, neste Anexo, aspectos relevantes e didáticos abordados no Curso "Avaliação de Controles Internos, Aula 2: Modelos de Referência para Controle Interno" acerca de controles internos.

As atividades de controle envolvem um vasto rol de controles preventivos e detectivos, a seguir exemplificados:

• **atribuição de autoridade e limites de alçada (prevenção)** - consiste em estabelecer competências e limites, de acordo com a posição hierárquica de unidades da estrutura organizacional e de governança ou as responsabilidades gerenciais de ocupantes de cargos e funções, quanto à possibilidade de autorizar, executar ou aprovar atos ou transações em nome da organização. É uma forma de assegurar que os atos administrativos sejam realizados por quem tem o respaldo da organização para efetivá-los;

• **procedimentos de autorização e aprovação (prevenção/detecção)** - Uma vez fixados os limites de alçada e as competências para exercê-los, a administração determina quais atividades ou transações necessitam de uma autorização e aprovação superior para que sejam efetivadas. A finalidade da autorização é assegurar que apenas os atos administrativos os quais a administração tem intenção de realizar sejam iniciados. A aprovação, de forma manual ou eletrônica, implica a validação do ato e certificação da conformidade com as políticas e os procedimentos estabelecidos pela organização.

Salvo nos casos de aprovação prévia de propostas (solicitações, pedidos, requisições, por exemplo), a aprovação é um procedimento posterior à realização de atos anteriormente autorizados. Os responsáveis pela aprovação normalmente verificam a documentação pertinente, questionam itens e asseguram-se de que os preceitos necessários à conformidade do ato estão checados, antes de darem a sua aprovação.

As políticas que instruem os procedimentos de autorização e aprovação devem ser formalmente estabelecidas e comunicadas a todos os gestores e funcionários e incluir as condições específicas e os termos segundo os quais eles devem ser realizados. Por sua vez, os procedimentos de autorização e aprovação devem ser formalizados e documentados nos processos ou sistemas onde ocorrerem;

• **segregação de funções ou atividades (prevenção)** - consiste na separação de atribuições ou responsabilidades entre diferentes pessoas em funções ou atividades-chave de autorização, execução, registro, custódia e revisão/ateste/aprovação ou auditoria. Tem por fim assegurar que indivíduos não realizem funções incompatíveis. As funções, por seu turno, reputam-se incompatíveis, quando, um mesmo indivíduo, em

virtude das atribuições que lhe foram imputadas, tem a possibilidade de ocultar um erro ou fraude por si cometida.

A segregação de funções reduz o risco de erros humanos e de ações indesejadas e o risco de não detectar tais ocorrências, muito embora o conluio entre pessoas possa reduzir ou destruir a eficácia desta atividade de controle. Exemplificando: quem é responsável pela guarda ou custódia de recursos financeiros não deve ser a mesma pessoa que tem poder para autorizar a movimentação desses recursos nem de registrar tais movimentos;

• **rotatividade de pessoas em funções (prevenção)** - significa impedir que a mesma pessoa seja responsável por atividades sensíveis por um longo período de tempo. Tem uma finalidade semelhante à segregação de funções, impedir que uma pessoa cometa um erro ou fraude e possa esconder a situação por muito tempo. A exigência de gozo de férias anuais tem o efeito de rotatividade temporária de funções;

• **revisões independentes, verificações e conciliações (detecção)** - consistem na revisão de atos ou transações por um terceiro, não envolvido na sua execução. Esse tipo de atividade de controle é muitas vezes utilizado para compensar a não adoção de outros controles preventivos ou detectivos, ou para contrabalançar outras falhas na estrutura de controle da organização como, por exemplo, a ausência de segregação de funções. Quando isso ocorre, o controle é denominado compensatório, embora, na essência, seja um controle detectivo.

As **verificações** ou conferências são controles básicos em qualquer atividade. As transações e os eventos significativos devem ser verificados antes e depois de ocorrerem. Exemplificativamente, no recebimento de produtos numa organização, o número de produtos entregues deve ser conferido com o número de produtos solicitados. Depois, o número de produtos faturados deve ser cotejado com o número de produtos recebidos. O inventário também é verificado quando se realizam balanços no almoxarifado.

As **conciliações** são atividades de controle que consistem em confrontar registros com documentos apropriados como, por exemplo, registros patrimoniais com relatórios de inventários de bens, registros contábeis de contas bancárias com extratos bancários correspondentes etc. Para serem efetivos, os procedimentos de conciliação devem ser periódicos e realizados com regularidade.

As diferenças encontradas numa conciliação devem ser devidamente explicadas, comprovadas e documentadas e os ajustes correspondentes, quando cabíveis, devem ser feitos nos registros e na contabilidade.

Observa-se, assim, que esse é um tipo de atividade de controle de grande importância para assegurar a confiabilidade dos registros que servem de base tanto para o processo decisório interno da organização como para o cumprimento das obrigações de *accountability*, ou seja, um dos objetivos do controle interno, conforme a Intosai e o Coso;

• **avaliações de desempenho operacional (detecção)** - permitem à administração verificar se os resultados obtidos estão alcançando os objetivos e padrões pré-

estabelecidos. As avaliações de desempenho operacional incluem **revisões da alta direção**, ao comparar o desempenho atual em relação ao orçado, às previsões, aos períodos anteriores e aos concorrentes, bem como a análise crítica de **indicadores de desempenho**, relacionando-se diferentes conjuntos de dados, sejam eles operacionais ou financeiros, em conjunto com a realização de análises dos relacionamentos e das medidas de investigação e correção;

• **avaliações de operações, processos e atividades (detecção)** - Consiste no aprofundamento de investigações resultantes de avaliações de desempenho operacional ou em avaliações periódicas para assegurar que operações, processos e atividades cumprem com regulamentos, políticas, procedimentos ou outros requisitos em vigor;

• **supervisão direta (prevenção/detecção)** - presente em todos os níveis da organização, consiste no acompanhamento do trabalho delegado aos funcionários pelo respectivo superior hierárquico. Inclui atividades de comunicação de atribuições, revisão e aprovação de trabalhos, bem como de orientação e treinamento do pessoal supervisionado para o desempenho das atribuições.

Para a INTOSAI (Organização Internacional de Entidades Fiscalizadoras Superiores), a supervisão compreende:

a. comunicação clara das funções e responsabilidades atribuídas a cada membro da equipe e da obrigação de prestar contas;

b. revisão sistemática do trabalho de cada membro na extensão necessária;

c. aprovação do trabalho nas etapas críticas para assegurar que flui como pretendido;

• **controles de acesso a recursos e registros (prevenção)** - os ativos críticos da organização devem ser protegidos contra desperdício, perda, mau uso, dano, utilização não autorizada ou apropriação indevida. Assim, a depender do risco percebido em relação a essas ocorrências, devem-se estabelecer controles para limitar o acesso a recursos e registros (computadores, estoques, títulos, dinheiro, registros, bens etc.) às pessoas autorizadas a sua guarda, conservação e controle, as quais devem ser obrigadas a prestar contas de sua custódia e utilização. Incluem-se dentre essas atividades, os controles físicos e lógicos de acesso (controles de entrada/saída de pessoas, veículos, bens e materiais; criptografia e senha de arquivos eletrônicos etc.), além de procedimentos de outorga de guarda/transferência de bens, complementados por inventários periódicos e comparação com registros patrimoniais e de controle.

ATIVIDADES DE CONTROLE ESPECÍFICAS PARA SISTEMAS DE TECNOLOGIA DA INFORMAÇÃO:

As organizações em todos os setores estão cada vez mais dependentes dos recursos de Tecnologia da Informação (TI) para conduzir os negócios, alcançar objetivos e cumprir suas missões. Um fator crítico dessa nova realidade é o uso eficiente e seguro desses recursos.

A informação e a tecnologia que lhe dá suporte é hoje, para a maioria das organizações, um ativo valioso. Em muitos casos, há uma dependência crítica dos processos organizacionais suportados por TI, exigindo-se uma adequada gestão de riscos e uma crescente necessidade de controle sobre as informações, fatores hoje considerados elementos-chave na governança corporativa.

Os **controles gerais de TI** abrangem a estrutura, as políticas e os procedimentos aplicáveis a todos os sistemas de informação da organização, incluindo a totalidade dos componentes, desde a arquitetura de processamento – servidores, redes, estações etc. – até ambientes de usuários finais, com a finalidade de ajudar a assegurar uma operação adequada e contínua. Eles criam o ambiente no qual operam os sistemas aplicativos. São seis as categorias principais de atividades de controle que precisam ser consideradas ao se avaliar os controles gerais de TI:

a. Programa de planejamento e gestão da segurança de TI;

b. Controles de acesso;

c. Controles de desenvolvimento, manutenção e mudança em sistemas;

d. Controles sobre aplicativos;

e. Segregação de funções;

f. Continuidade dos serviços.

Os **controles de aplicativos de TI** abrangem a estrutura, as políticas e os procedimentos diretamente relacionados aos aplicativos corporativos individuais, incluindo procedimentos embutidos no código do programa, com a finalidade de ajudar a assegurar a integridade, precisão, autorização e validade de dados e transações neles processados. São quatro as categorias principais de atividades de controle que precisam ser consideradas ao se avaliar os controles de aplicativos de TI:

a. Controles de autorização;

b. Controles de integralidade;

c. Controles de precisão;

d. Controles de integridade do processamento e dos arquivos de dados.

Os controles gerais e os controles de aplicativos de TI, em conjunto com processos de controle manual, quando necessários (como políticas e procedimentos associados a atividades de usuários), devem se inter-relacionar. Todos são necessários para assegurar a integridade, a precisão e a validade das informações.

ANEXO III
Roteiro Básico para o Processo de Gerenciamento de Riscos
(REFERENCIAL BÁSICO DE GESTÃO DE RISCOS DO TCU)

1) Que empreendimento você deseja proteger ou ver bem-sucedido? Pode ser um projeto, um processo, um departamento, uma organização, uma política.

2) Quais são os objetivos desse empreendimento?

3) Que fatores (fraquezas, ameaças, erros, falhas...) podem afetar o alcance desses objetivos?

4) Que riscos podem se originar da ocorrência desses fatores?

5) Qual seria a probabilidade e o impacto da ocorrência de cada um desses riscos se nada tivesse sido feito para mitigá-los até o momento? Calcule o nível de risco inerente (probabilidade inicial x impacto inicial).

6) Qual é o apetite e a tolerância a risco do seu Órgão? Qual nível de risco ele considera aceitável?

7) Quais medidas mitigadoras já foram adotadas e que controles internos já estão implantados? Qual a eficácia dessas medidas e controles? Algum deles pode ser eliminado?

8) Que outras medidas mitigadoras e controles internos podem ser adotados para adequar o nível de risco ao apetite e à tolerância a risco?

9) Qual é a probabilidade e o impacto esperado da ocorrência desses riscos após a avaliação de eficácia e adequação das medidas mitigadoras e controles internos? Calcule o nível de risco residual (nível de risco inerente x risco de controle).

10) Com que frequência esses riscos devem ser monitorados?

11) Quem são os responsáveis por monitorar os riscos? Quem deve ser comunicado acerca desses? Com que frequência isso deve ser feito e por quais mecanismos?

ANEXO IV
Roteiro Prático para o Processo de Gerenciamento de Riscos no TRE-BA

CONTEXTO ESPECÍFICO

1) Identificar o processo organizacional que será submetido ao processo de gerenciamento de riscos (preencher o mapa do processo, que corresponde à Tabela 4 – Estabelecimento do Contexto Específico, exceto os campos relativos ao Fluxo do Processo);

2) Levantar as atividades do processo organizacional que será submetido ao processo de gerenciamento de riscos e seus respectivos responsáveis, podendo, em seguida, desenhar o fluxo correspondente (preencher os campos "Fluxo do Processo" da Tabela 4 – Mapa do Processo - Estabelecimento do Contexto Específico);

3) Levantar o ambiente do processo organizacional que será submetido ao processo de gerenciamento de riscos, identificando as ameaças e oportunidades, forças e fraquezas que o circundam (preencher a Tabela 5 – Matriz SWOT);

IDENTIFICAÇÃO

4) Preencher os campos "Processo Organizacional", "Atividade" e Responsável/Atividade todos da Tabela 6 – Identificação de Riscos, com as informações lançadas nos campos equivalentes da Tabela 4 – Mapa do Processo - Estabelecimento do Contexto Específico;

5) Identificar as principais funções ou objetivos do processo, ambiente, projeto ou sistema: com base na descrição de processos, ambientes, projetos ou sistemas, o primeiro passo é identificar as principais funções e objetivos que devem ser cumpridos pelo objeto que está sendo examinado quanto aos riscos (preencher o campo "Objetivo/Finalidade" da Tabela 6 – Identificação de Riscos);

6) Levantar possíveis eventos que podem impedir ou dificultar a execução ou o atingimento dos objetivos do processo, ambiente, projeto ou sistema: conhecendo a função e os objetivos de determinado processo, ambiente, projeto ou sistema, torna-se possível identificar o que poderia impactar negativamente a consecução dos objetivos e a inexecução de funções (preencher o campo "Evento de Risco" da Tabela 6 – Identificação de Riscos);

7) Levantar as possíveis causas que levam à ocorrência do evento: Após a identificação dos eventos de risco que podem impedir ou dificultar o correto funcionamento de um processo, ambiente, projeto ou sistema, é necessário levantar o que está ocasionando a materialização desses eventos: são as chamadas causas do risco. As causas podem ter diversas origens tanto internas quanto externas à organização (o que pode ser evidenciado por meio de uma Análise SWOT), podendo advir, exemplificadamente, de falhas humanas, falhas de processos e sistemas, vulnerabilidades sem o devido controle, ação intencional de agentes que exploram tais vulnerabilidades, eventos naturais, dentre outras origens (preencher o campo "Causa" da Tabela 6 – Identificação de Riscos);

8) Levantar as possíveis consequências da ocorrência do evento (levando em consideração os objetivos organizacionais e conformidade normativa): Por fim, a etapa

IDENTIFICAÇÃO

de identificação de riscos deve levantar os potenciais impactos e consequências para os objetivos organizacionais advindos da ocorrência dos eventos de riscos levantados. O levantamento de consequências basicamente se refere a dois pontos na gestão de riscos: a consecução dos objetivos organizacionais (ou somente do processo analisado, ou do projeto, ou do sistema) e a manutenção de conformidade com a legislação e aparato normativo vigente (preencher o campo "Consequência" da Tabela 6 – Identificação de Riscos);

9) Identificar a categoria de risco dentre aquelas categorias previstas no art. 5º, da Resolução Administrativa nº 16/2018, bem como no Plano de Integridade do Ministério da Transparência e da Controladoria-Geral da União, aprovado pela Portaria nº 1.075, de 23 de abril de 2018, quais sejam, riscos estratégicos, riscos operacionais, riscos de conformidade, riscos de imagem, riscos-chave e riscos à integridade (preencher o campo "Categoria de Risco" da Tabela 6 – Identificação de Riscos);

ANÁLISE

10) Definir a probabilidade de ocorrência do evento de risco (preencher o campo "probabilidade" na Tabela 10 – Análise de Riscos Inerentes e na Tabela 12 – Análise de Riscos, com base nos parâmetros contidos na Tabela 7 – Escala de Probabilidade);

11) Definir o impacto das consequências advindas da materialização do evento de risco em análise (preencher o campo "Impacto" na Tabela 10 – Análise de Riscos Inerentes e na Tabela 12 – Análise de Riscos, com base nos parâmetros contidos na Tabela 8 – Escala de Impacto);

12) Calcular o risco inerente, multiplicando a probabilidade e o impacto do risco em análise (preencher o campo "Risco Inerente" na Tabela 10 – Análise de Riscos Inerentes e na Tabela 12 – Análise de Riscos com o produto da multiplicação entre a probabilidade de ocorrência do evento e o impacto de suas consequências caso se concretize conforme se pode visualizar ilustrativamente na Tabela 9 – Matriz Impacto X Probabilidade – Nível de Risco Inerente);

13) Identificar os controles internos preexistentes, bem como o respectivo responsável pela sua execução (preencher os campos "Controles Internos" e "Responsável", ambos da Tabela 12 – Análise de Riscos);

14) Indicar o nível de confiança do controle (preencher o campo "Avaliação do Controle/ Nível de Confiança" da Tabela 12 – Análise de Riscos, a partir dos critérios definidos na Coluna 1-Nível de Confiança da Tabela 11 - Avaliação do Risco do Controle);

15) Avaliar o risco do controle interno, a partir dos critérios definidos na Tabela 11 – Avaliação do Risco do Controle (preencher o campo "Risco do Controle" da Tabela 12 – Análise de Riscos com o valor atribuído ao risco do controle analisado conforme parâmetros consignados na Tabela 11 – Avaliação do Risco do Controle");

16) Calcular o risco residual, multiplicando o risco inerente em análise pelo valor do risco do controle (preencher o campo "Risco Residual" da Tabela 12 – Análise de Riscos com o produto da multiplicação entre risco inerente e risco do controle).

AVALIAÇÃO

17) Classificar o valor do risco residual calculado dentre os parâmetros definidos na Tabela 13 – Escala para Classificação de Níveis de Risco (preencher o campo "Classificação do Risco Residual" da Tabela 15 – Avaliação de Riscos, a partir dos parâmetros estabelecidos na Tabela 13 - Escala para classificação de níveis de risco);

18) Cotejar os níveis de riscos classificados com o apetite a risco da organização para identificar a diretriz para resposta, de modo a indicar o tratamento adequado na fase seguinte (preencher o campo "Diretriz para Resposta" da Tabela 15 – Avaliação de Riscos, de acordo com os parâmetros estabelecidos na Tabela 14 – Diretrizes para Resposta).

TRATAMENTO

19) Identificar a resposta ao nível de risco residual classificado (preencher o campo "Resposta ao Risco" da Tabela 17 – Tratamento de Riscos, a partir dos parâmetros estabelecidos na Tabela 16 – Respostas a Riscos);

20) Indicar as ações de tratamento selecionadas para adequar o nível de risco residual classificado para o limite aceitável pelo TRE-BA, isto é, para amoldá-lo ao apetite a risco do Órgão (preencher o campo "Ações de Tratamento" da Tabela 17 – Tratamento de Riscos com controles internos adicionais selecionados pelo gestor de riscos);

21) Indicar o responsável pela implementação das ações de tratamento selecionadas (preencher o campo "Responsável" da Tabela 17 – Tratamento de Riscos);

22) Indicar o prazo para implementação das ações de tratamento selecionadas (preencher o campo "Prazo para implementação" da Tabela 17 – Tratamento de Riscos);

23) Indicar a data para iniciar a implementação da ação de tratamento selecionada (preencher o campo "Data Inicial" da Tabela 17 – Tratamento de Riscos);

MONITORAMENTO

24) Indicar o estágio da ação de tratamento: a iniciar, em andamento ou concluída (preencher o campo "Andamento da Ação de Tratamento" da Tabela 18 – Monitoramento de Riscos);

25) Indicar as formas de monitoramento: indicadores, nesse caso anotar a fórmula de medição, auditorias, relatórios, etc. (preencher o campo "Monitoramento" da Tabela 18 – Monitoramento de Riscos).

26) As atividades de comunicação e consulta devem permear todo o processo de gerenciamento de riscos, visando à disseminação das informações produzidas. Para auxiliar o desenvolvimento dessas atividades, poderá ser preenchido o Plano de Comunicação cujo modelo constitui a Tabela 19 – Comunicação e Consulta deste documento.

ANEXO V

Formulário – Matriz de Identificação, Análise, Avaliação, Tratamento e Monitoramento de Riscos

PROCESSO:

OBJETO DO PROCESSO:

IDENTIFICAÇÃO									ANÁLISE								AVALIAÇÃO		TRATAMENTO E MONITORAMENTO							
Nº	Processo Organizacional	Atividade	Objetivo/Finalidade	Responsável/atividade	Evento de Risco	Causas	Consequências	Categoria de Risco	Probabilidade	Impacto	Risco Inerente	Controles Internos	Responsável	Nível de confiança	Risco do Controle	Risco Residual	Classificação do Risco	Diretrizes para resposta	Resposta ao Risco	Ações de Tratamento	Responsável	Prazo para implementação	Data Inicial	Meta	Andamento da Ação de Tratamento	Monitoramento
1											0					0										
2											0					0										
3											0					0										
4											0					0										
5											0					0										
6											0					0										
7											0					0										
8											0					0										
9											0					0										
10											0					0										
11											0					0										
12											0					0										
13											0					0										
14											0					0										
15											0					0										
16											0					0										
17											0					0										
18											0					0										
19											0					0										
20											0					0										

ANEXO VI

Exemplo de Plano de Tratamento de Riscos Editado – 1 linha do PTR

PROCESSO:	Recadastramento Biométrico Extraordinário
OBJETIVO DO PROCES	Realizar o recadastrmaento biométrico extraordinário

IDENTIFICAÇÃO									**ANÁLISE**		
Nº	**Processo Organizacional**	**Atividade**	**Objetivo/Finalidade**	**Responsável/atividade**	**Evento de Risco**	**Causas**	**Consequências**	**Categoria de Risco**	**Probabilidade**	**Impacto**	**Risco Inerente**
1	Recadastramento Biométrico Extraordinário	Atendimento ao Eleitor	Atender adequadamente o eleitor realizando coleta de dados biométricos com qualidade	Cartório Eleitoral	Formação de longas filas	Insuficiência de pessoal; Estrutura inadequada; Atraso nas contratações; Deficiência de planejamento; Curto prazo para a biometria; Cultura do eleitor quanto ao comparecimento somente nos últimos dias de prazo; Concentração maior de divulgação na mídia nos últimos dias de prazo.	Insatisfação do eleitor; Dano à imagem do Tribunal; Cadastramento realizado de forma inadequada em razão da sobrecarga de trabalho dos atendentes; Adoecimento dos servidores.	Estratégico/Imagem /Chave	10	10	100

ANÁLISE					**AVALIAÇÃO**		**TRATAMENTO E MONITORAMENTO**							
Controles Internos	**Responsável**	**Nível de Confiança**	**Risco do Controle**	**Risco Residual**	**Classificação do Risco**	**Diretrizes para resposta**	**Resposta ao Risco**	**Ações de Tratamento**	**Responsável**	**Prazo para implementação**	**Data Inicial**	**Meta**	**Andamento da Ação de Tratamento**	**Monitoramento**
Requisição de servidores de outros órgãos das esferas municipal, estadual e federal; realização de convênios com órgãos públicos para ampliar a capacidade de atendimento; divulgação das informações de interesse do eleitor; planejamento e execução antecipada das contratações relacionadas à estrutura da biometria; triagem na fila; criação de postos de atendimento	Cartórios Eleitorais; Comissão de Biometria;	3	0,6	60	Alto	Tratar	Mitigar	Propor formalização de plano de divulgação com vistas a antecipar a procura do eleitor pelos serviços de cadastramento biométrico; Propor o aperfeiçoamento da triagem na fila da biometria; Estudar ampliação de convênios e da criação de postos de atendimento; Propor a adequação do prazo da revisão biométrica à demanda de eleitorado a biometrizar; Realizar deslocamento temporário de servidores lotados em outras unidades para suporte nas zonas eleitorais em biometria extraordinária.	ASCOM/Cartório Eleitoral;Comissão de Biometria	90 dias	25/02/2019	Risco baixo/muito baixo (ao menos 9,99)	A iniciar	

*(PTR editado, constante no Relatório de Gestão 2018, elaborado pela Comissão de Biometria. *Monitoramento não preenchido - tratamentos s não iniciados)*

Missão

Garantir a legitimidade do processo eleitoral e o livre exercício do direito de votar e ser votado, a fim de fortalecer a democracia.

Visão

Ser reconhecido como uma instituição pública independente e imparcial, referência na prestação de serviços e na conscientização para a cidadania.

Valores Organizacionais

Ética

Imparcialidade

Transparência

Respeito ao Ser Humano

Responsabilidade Socioambiental