2023

METODOLOGIA DE AVALIAÇÃO DE RISCOS E CONTROLES INTERNOS

Ministério das Cidades

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

Ministério das Cidades

Chefe da Assessoria Especial de Controle Interno
Fabiana Vieira Lima

Coordenadora-Geral de Controle Interno
Jeanne Kettlin Alves Marques de Medeiros

Izabella da Silva Rufino
Coodenadora de Riscos e Controle Interno

Elaboração
Denise Rodrigues dos Santos

Ano 2023 - Versão 01

Sumário

Metodologia de Avaliação de Riscos e Controles Internos

CAP. 01 – Introdução

O processo de avaliação de riscos e controles internos definido nesta metodologia está aderente às diretrizes definidas na Política de Gestão de Riscos e Controles Internos do Ministério das Cidades - MCID, aprovada pelo Comitê Interno de Governança (Cigov).

O modelo adotado é estruturado considerando o Modelo das Três Linhas, de forma a melhor esclarecer os papéis e as responsabilidades de cada um no gerenciamento de riscos e controles, tendo como base conceitos, diretrizes e princípios do *Committee of Sponsoring Organizations of the Treadway Commission* - COSO; da ABNT NBR ISO 31.000 e da Instrução Normativa Conjunta nº 1, de 10 de maio de 2016 da Controladoria-Geral da União e do extinto Ministério do Planejamento, Desenvolvimento e Gestão.

O foco das avaliações está pautado na contribuição que uma gestão eficiente de riscos e controles internos fornece para o alcance dos objetivos propostos. Para tanto, visa identificar e tratar os riscos relevantes e identificar controles capazes de trazer um balanceamento adequado entre riscos e controles, dando mais segurança no desenvolvimento das atividades e eliminando aqueles que não agregam valor.

Portanto, a gestão de riscos aumenta a capacidade em lidar com incertezas, estimula a transparência e o uso eficiente, eficaz e efetivo dos recursos públicos, favorecendo o cumprimento dos objetivos e competências do Ministério das Cidades e de suas unidades.

A metodologia tem abrangência para o Ministério das Cidades, com indicação de utilização por todas as unidades, de forma a promover uma linguagem única de riscos e controles.

As seguintes etapas são necessárias para a avaliação de riscos e controles:

I. Análise de ambiente e dos objetivos;
II. Identificação dos riscos;
III. Avaliação dos riscos;
IV. Resposta aos riscos; e
V. Monitoramento e Comunicação.

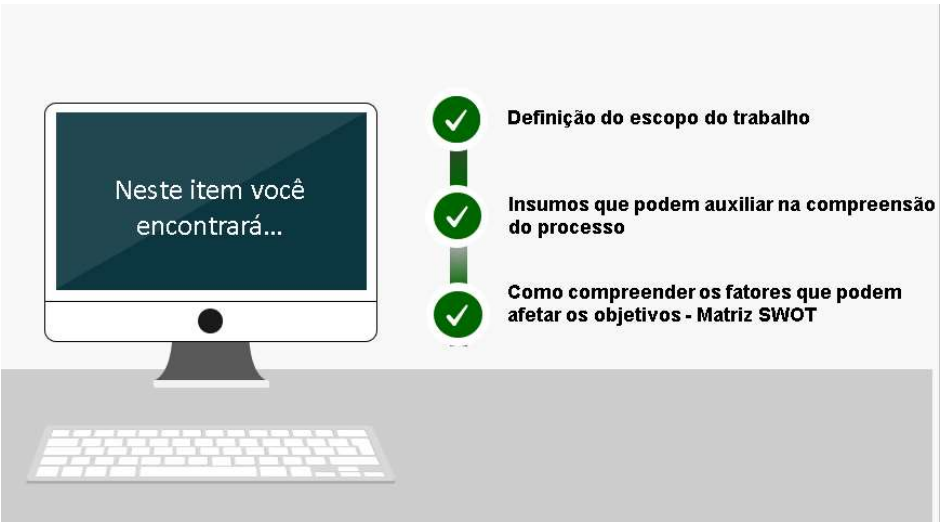
Ao longo deste documento serão detalhadas cada uma dessas etapas, com proposição de eventuais técnicas complementares, de forma a estruturar o método para avaliação dos riscos e dos controles internos.

Cumpre informar que para a implementação do gerenciamento de riscos será utilizado o sistema informatizado denominado Ágatha para documentar as etapas que compreendem a avaliação de riscos e controles. (Endereço eletrônico: https://agatha.mdr.gov.br/#)

Para a etapa de Resposta aos Riscos e Monitoramento dos controles propostos no Plano de Controle será utilizado o sistema e-Aud. (Endereço eletrônico: https:// https://eaud.cgu.gov.br/).

CAP. 02 – Etapas da Avaliação de Riscos e Controles Internos

I. Análise do Ambiente e dos Objetivos



Esta etapa trata do levantamento e registro dos aspectos externos e internos, com a finalidade de cumprir os objetivos institucionais, permitindo a compreensão clara do ambiente em que o objeto a ser avaliado se insere e, principalmente, identificar os fatores que podem influenciar a capacidade de atingir os resultados planejados.

Definição do Escopo do Trabalho

É de fundamental importância definir o escopo do trabalho, ou seja, o objeto a ser avaliado. Por exemplo, no caso de avaliação de um processo, a partir de qual etapa ou atividade e até qual fase será feita a avaliação. Desse modo, fica claro qual será o escopo do objeto da gestão de riscos.

Necessitam ser abordados também alguns insumos que podem ser consultados, de acordo com o trabalho a ser realizado, visando um melhor entendimento do processo e de possíveis fragilidades existentes.

Insumos

Deve ser considerada a motivação pelo qual a avaliação foi indicada, a fim de dar foco aos motivos da priorização, a exemplo de quando a avaliação decorre da aplicação dos Critérios para Priorização de Processos.

Além do resultado da Priorização de Processos, se for o caso, outros insumos podem auxiliar na compreensão do processo e deverão ser observados, tais como:

- mapeamento do processo – fluxograma;
- normatização clara e atualizada sobre as atividades do processo;
- centralização de conhecimento de atividades complexas em apenas um profissional;
- atividades predominantemente manuais, que poderiam ser automatizadas;

- apontamentos por órgãos externos, tais como Controladoria Geral da União (CGU) e Tribunal de Contas da União (TCU);
- reclamações ou denúncias registradas na Ouvidoria;
- processos judiciais;
- avaliação de ciclos anteriores;
- Tomadas de Contas Especiais e suas causas.

Deve, também, ser detalhado e delimitado o objeto a ser avaliado, levando em consideração a identificação dos envolvidos, o objetivo do processo/projeto/iniciativa, os sistemas disponíveis para sua utilização e seu cronograma de execução.

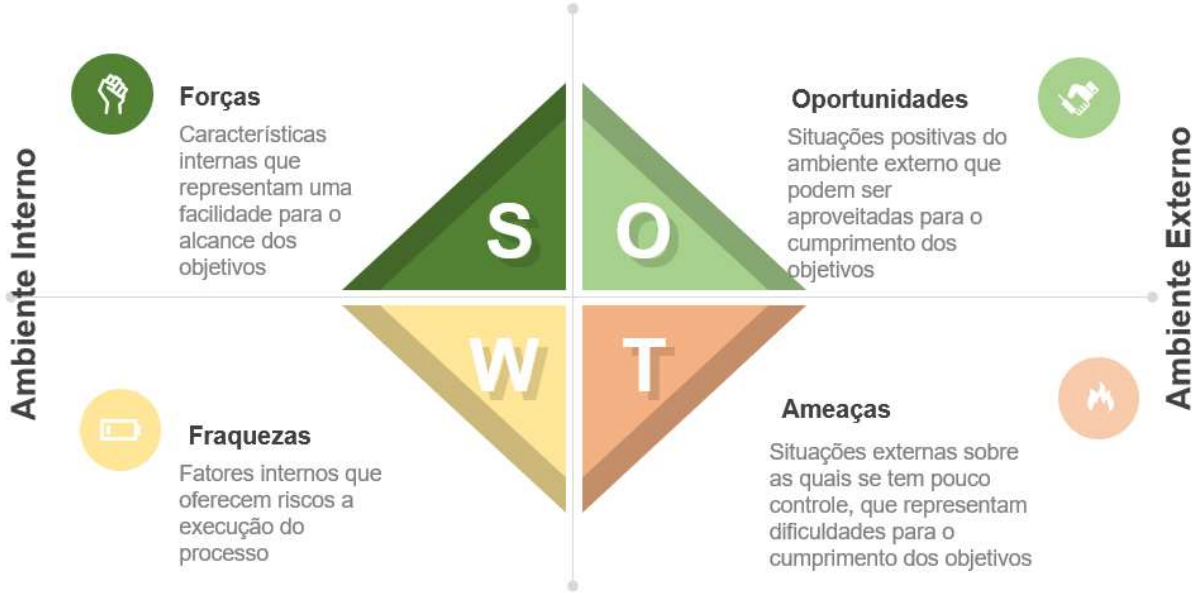
Caso necessário, propomos a utilização da Matriz SWOT (documento disponível no Anexo I), ferramenta para auxiliar no levantamento das Forças, Fraquezas, Oportunidades e Ameaças que podem afetar o objetivo do objeto que está sob avaliação.

Matriz SWOT

A análise SWOT é um dos instrumentos mais consagrados de planejamento, voltada para a análise dos ambientes internos e externos das organizações, atividade fundamental para a definição da estratégia. No que se refere ao ambiente interno são identificadas as forças e fraquezas que a organização possui. Quanto ao ambiente externo, são identificadas as oportunidades e ameaças, eventos que, caso ocorram, podem impactar positivamente ou negativamente a atuação da organização.[1]

Poderá ser realizada análise SWOT para identificação dos pontos fortes e fracos do ambiente interno (próprio do MCID), as oportunidades e ameaças do ambiente externo ao Ministério, e a identificação dos principais atores envolvidos no processo referentes ao gerenciamento de riscos e controles, com a finalidade de melhor compreender os fatores que podem afetar o objeto a ser avaliado.

Figura 01 – Matriz SWOT



Fonte: Manual de Gestão de Riscos, Controles Internos e Integridade do Ministério do Desenvolvimento Regional - 1ª Edição – 2020, com Adaptações.

[1] Fonte: Plano Estratégico Institucional MDR: Sumário Executivo 2020-2023

Na prática, a análise SWOT permite:

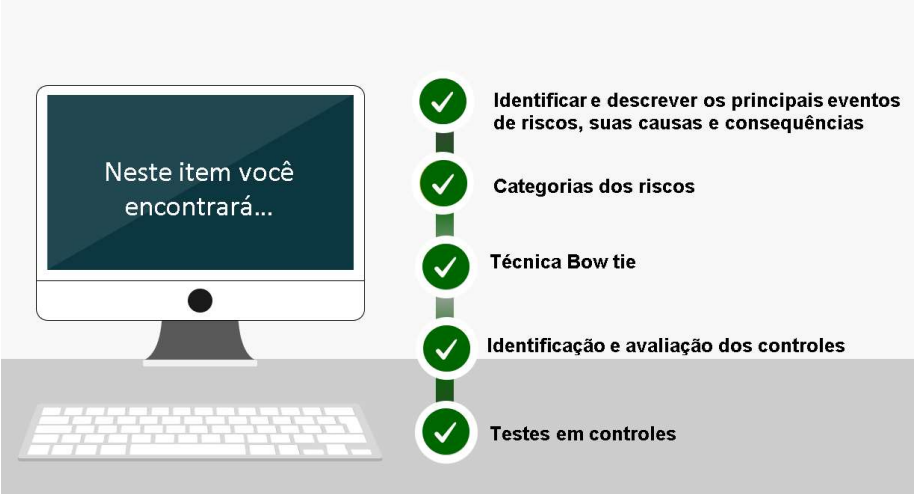
Forças e Oportunidades: tomar consciência dos pontos fortes para aproveitar ao máximo as oportunidades identificadas.

Forças e Ameaças: conhecer os pontos fortes que possam minimizar os efeitos das ameaças identificadas.

Fraquezas e Oportunidades: minimizar os efeitos negativos de pontos fracos e em simultâneo aproveitar as oportunidades identificadas.

Fraquezas e Ameaças – adotar estratégias para minimizar ou ultrapassar os pontos fracos e, tanto quanto possível, fazer frente às ameaças.

II. Identificação dos Riscos



A etapa de identificação dos riscos envolve o reconhecimento, a descrição e o registro dos eventos de riscos mais relevantes, com a caracterização de suas prováveis causas e possíveis consequências. Nesta etapa deverá ser desenvolvida uma lista de eventos de riscos que podem comprometer os resultados e o alcance dos objetivos do processo, projeto, programa, atividade ou iniciativa, objeto da avaliação de riscos, que tenha o potencial de afetar o valor público a ser entregue à sociedade.

Na sequência são identificados e avaliados os controles existentes para cada um dos eventos relacionados, de forma a verificar se estão proporcionando a redução dos riscos e sua manutenção a níveis considerados adequados pela alta administração.

Poderá haver a realização de testes, visando certificar a efetividade de algum controle.

Perguntas Relevantes para a Identificação dos Riscos

A depender da característica do objeto a ser avaliado, algumas perguntas podem auxiliar na identificação dos eventos de riscos:

- O que pode dar errado?
- O que pode nos levar à falha?

- Quais os principais pontos de vulnerabilidade?
- Como alguém poderia fraudar ou roubar?
- As informações são restritas e protegidas?
- As informações são automatizadas?
- Como podemos saber se estamos alcançando nossos objetivos?
- Quais atividades têm maior grau de complexidade?
- Existem atividades complexas concentradas em apenas uma pessoa?
- Onde são tomadas as decisões mais complexas e relevantes?
- A competência técnica e administrativa é observada?
- O que pode gerar perda?
- O que pode gerar retrabalho?
- O que pode ocasionar dano a imagem?
- Existe algum impedimento legal para prosseguimento da atividade?
- A segregação de funções é obedecida?
- Quais gargalos podem comprometer a entrega?
- Existe disponibilidade de pessoas capacitadas para cuidar do assunto?
- A equipe conhece toda a legislação, manuais, etc que tratam do assunto?
- Há disponibilidade orçamentária?
- As informações são claras, suficientes e disponíveis para a tomada de decisão?
- Existe alguma recomendação dos órgãos de controle, processos judiciais ou reclamações e denúncias na Ouvidoria relacionados aos processos?

Categorias dos riscos: a classificação do evento de risco deverá observar aspectos subdivididos nas 5 categorias[2] a seguir:

- **Operacional**: eventos que podem comprometer as atividades do Ministério, normalmente, associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas. Esta definição inclui o risco legal.[3]
- **Orçamentário**: eventos que podem comprometer a capacidade do Ministério de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária;
- **Imagem**: eventos que podem comprometer a confiança da sociedade em relação à capacidade do Ministério em cumprir sua missão institucional;
- **Conformidade**: eventos derivados de descumprimento legislativo ou normativo que podem comprometer as atividades do Ministério;
- **Integridade**: eventos relacionados a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer valores e padrões preconizados pelo Ministério e a realização de seus objetivos; e
- **Estratégico**: eventos que podem comprometer a estratégia do Ministério devido a mudanças

[2] Categorização foi baseada na Metodologia de Gestão de Riscos do Ministério do Desenvolvimento Regional.
[3] Conceito adaptado da Resolução Bacen nº 4.557, DE 23/02/2017 que dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital.

no ambiente interno ou externo, consideração de premissas inadequadas ou falhas na execução de iniciativas estratégicas.

Caso o evento de risco esteja associado a duas ou mais categorias, deverá ser avaliada a necessidade de identificação dos dois riscos ou indicar a categoria que mais representa aquele risco. O risco de integridade é o único que permite a associação com outro risco.

Bow Tie

A técnica *Bow Tie*, figura 2, possibilita registrar de forma estruturada as informações de identificação do evento de risco, suas causas e consequências. Deverá ser utilizado um Bow Tie para cada evento de risco identificado. O arquivo contendo o Bow Tie completo está disponível no Anexo II.

Figura 2: Bow Tie Adaptado – Parte Riscos

Identificação e avaliação dos controles

Controle inclui qualquer norma, check list, processo, política, dispositivo, prática ou outra ação ou medida adotada, com o potencial de mitigar um risco. Por esse motivo os controles devem ser dimensionados a um nível compatível com o grau do risco identificado, devendo ser aprimorados a depender da elevação das vulnerabilidades. Os controles têm a finalidade de reduzir os riscos a níveis considerados adequados pela alta administração.

As atividades de controle ocorrem por todo o órgão, em todos os níveis e em todas as funções, desde a concepção da estratégia até a execução dos processos. Elas consideram os limites das atividades nos diversos níveis de aprovação, autorização, verificação, segregação de funções, entre outras, motivo pelo qual, além da avaliação dos riscos há necessidade de serem avaliados os controles.

Quando não é possível a implementação de um controle em função da sua complexidade, alto custo, etc, deve-se avaliar a instituição de um controle compensatório, com o objetivo de mitigar o risco até a implementação de um controle definitivo.

Classificação dos Controles: um controle pode ser classificado em corporativo ou operacional.

Controles Corporativos:

Os controles corporativos, ou controles em nível de entidade (ELC – Entity Level Controls), são controles que asseguram a realização das diretrizes da organização. Eles podem ser indiretos (ELC Indireto), tais como Políticas, normas, Código de Ética, treinamentos; ou diretos (ELC Direto), geralmente são controles com características de monitoramento com emissão de relatórios gerenciais.

Os controles em nível de entidade auxiliam na mitigação dos riscos, no entanto, tem precisão menor do que os controles operacionais.

Controles Operacionais:

Os controles operacionais são os controles que afetam de forma mais direta o processo. São chamados também de controles transacionais, visto serem procedimentos ou atividades que objetivam a mitigação de fatores de risco identificados nos processos.

Identificação de controles

Devem ser identificados controles existentes para cada um dos eventos relacionados na identificação de riscos.

Orienta-se que todo o processo de gestão de riscos observe os controles sob a ótica de custo e benefício, de forma a otimizar a alocação de recursos e permitir maior alcance do valor público gerado. A exceção de atividades mandatórias, o custo de um controle não deve superar o benefício gerado ou esperado.

Nesta fase, deve-se avaliar também a existência de controles desnecessários ao processo, promovendo sua eliminação.

O quadro a seguir relaciona alguns exemplos de controles:

Quadro 01 – Exemplos de Controles

Exemplos de Controles			
Acompanhar	Comunicar	Fiscalizar	Ratificar
Alçada	Conciliar	Impedir	Reportar
Analisar	Conferir	Indicador	Revisar
Aprovar	Confirmar	Informar	Rodiziar
Atribuir	Contingenciar	Inspecionar	Segregar
Autenticar	Controlar	Instituir	Separar
Autorizar	Deferir	Monitorar	Testar
Avaliar	Definir	Normatizar	Travar
Bloquear	Divulgar	Padronizar	Treinar
Capacitar	Estabelecer	Parametrizar	Validar
Comparar	Examinar	Rastrear	Verificar

Características dos controles: os controles possuem várias características, como a seguir:

Quanto à Função:

Quadro 02 – Função dos Controles

Função dos Controles	
Preventivos	Tem como objetivo prevenir a materialização do evento de risco, atuando sobre as causas do risco e reduzindo a frequência de materialização de eventos.
Detectivos	Atuam na detecção da materialização do risco, sem impedir sua ocorrência. No entanto, permitem a gestão por meio de ações corretivas.

Quanto ao Tipo:

Quadro 03 – Tipos de Controles

Tipos de Controles		Exemplos
Automatizados	controles realizados por um sistema, sem intervenção humana em seu processamento	Sistema que faz a verificação de acesso por meio da senha do usuário
Informatizados	controles realizados por meio de planilhas, podendo ter fórmulas ou algum grau de automação	Planilhas composta pela imposição de dados, com células contendo algum tipo de fórmula ou automação
Manuais	controles realizados por pessoas	Segregação de funções, conferência, autorização

Avaliação dos controles

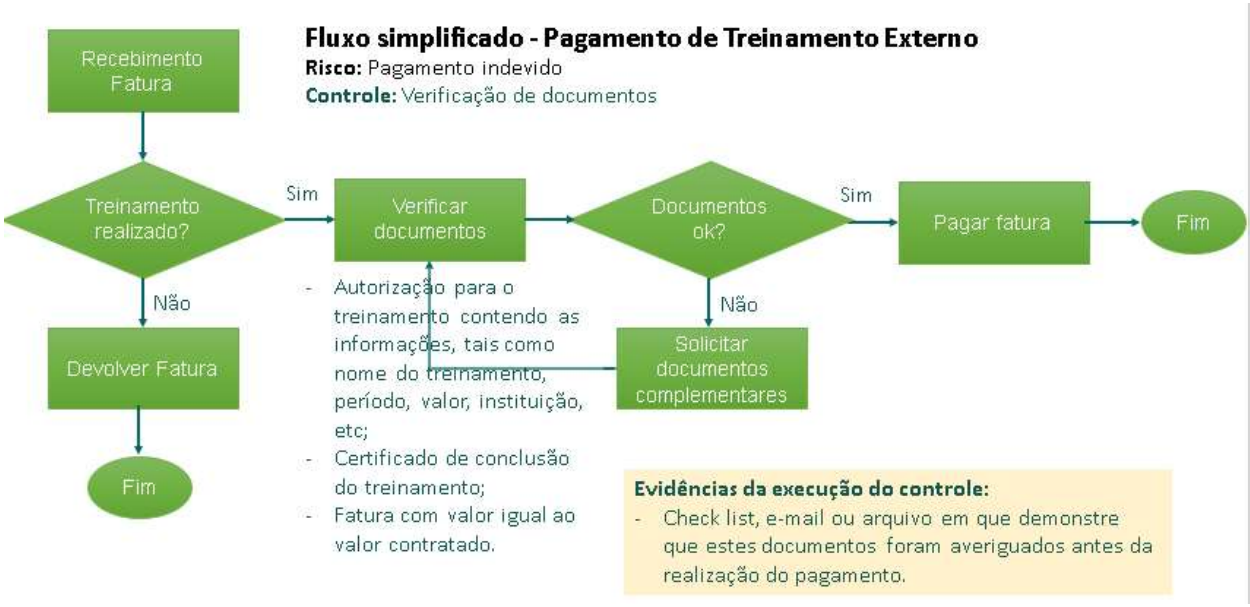
Visa avaliar os controles com relação ao desenho e à operação, de forma a verificar sua eficácia, conforme critérios definidos no Quadro 4, que observa a existência, formalização e suficiência, a fim de aferir o nível de risco aceitável ao processo em análise.

Quadro 04 – Avaliação dos Controles

Avaliação dos Controles	
Desenho **Há procedimento de controle suficiente e formalizado?**	**Operação** **Há procedimento de controle sendo executado? Há evidências de sua execução?**
1. há procedimentos de controle, mas insuficientes e não formalizados	1. há procedimentos de controle, mas não são executados
2. há procedimentos de controle formalizados, mas insuficiente	2. há procedimentos de controle formalizados, mas parcialmente executados
3. há procedimentos de controle suficientes, mas não formalizados	3. há procedimentos de controle suficientes, mas não evidenciados
4. há procedimentos de controle suficientes e formalizados	4. há procedimentos de controle executados de forma evidenciável

Evidência dos controles: as evidências podem ser obtidas por meio de relatórios, impressão de telas ou outros documentos que comprovem a execução dos controles existentes. Não se trata de comprovar se determinada atividade foi realizada, e sim, evidenciar se os controles para a realização da atividade foram executados.

Exemplo:



Dados não estruturados (DnE): Dados não-Estruturados são atividades ou controles realizados por meio de planilhas eletrônicas, sistemas, bancos de dados e outras soluções, que necessitam de organização, ajustes ou configuração para que possam gerar informações para tomada de decisões.

Até que o processo disponha de solução tecnológica corporativa e robusta, o gestor deve implementar controles compensatórios para reduzir riscos operacionais no uso de dados não estruturados.

A avaliação dos controles aplicados sobre DnE deve ser realizada quando relevante para o processo em análise, auxiliando na resposta quanto à avaliação da operação do controle.

Esses controles são avaliados a partir da comparação com a lista de requisitos necessários para dar certa segurança aos procedimentos, conforme o Quadro 05 e Anexo III:

Quadro 05 – Avaliação de Dados não Estruturados

Requisitos	Descrição
Controle de acesso	Planilha: Verificar se a planilha possui senha de proteção de acesso e é arquivada e utilizada em diretório de rede com controle de acesso, mediante a análise dos logs de acesso fornecidos pela área de TI Aplicativo: Verificar se o banco de dados restringe o acesso às informações mediante senha
Controle de mudanças	Verificar se as mudanças realizadas no sistema possuem registro passível de rastreamento (LOG)
Documentação	Verificar se os procedimentos usados para operacionalizar a planilha estão documentados
Acurácia e integridade de dados	Verificar se são efetuadas conciliações formais dos dados de entrada e de saída (resultados), que assegurem a abrangência, a consistência, a integridade e a confiabilidade deles. Essas conciliações devem ser documentadas e realizadas por funcionário diferente daquele que utiliza a base de dados
Validação lógica	Verificar se existe procedimento de revisão da lógica implementada na planilha por funcionário diferente daquele que a desenvolveu. Essa revisão deve ser documentada. (Ex:. cópias das mensagens de correio eletrônico com a descrição das alterações efetuadas pelo funcionário responsável e a confirmação da validação dessas alterações por outro funcionário)
Proteção lógica	Averiguar se foi implementada a proteção de células sensíveis da planilha, como as que contêm dados principais para o processamento e fórmulas

Após a identificação e avaliação dos controles, dá-se continuidade ao registro das informações no Bow Tie, conforme o Quadro 06. O Bow Tie completo encontra-se no Anexo II deste documento.

Quadro 06 -Bow Tie Adaptado – Parte Controle

Controles Internos						
Nome do Controle	Tipo de Controle			Descrição/Objetivo do controle	Desenho	Operação

Testes nos controles

Caso o resultado da avaliação dos controles pela área gestora tenha identificado algum tipo de fragilidade que denote a necessidade de aprimoramento, não há necessidade de a AECI realizar testes adicionais.

No entanto, caso na avaliação dos controles o gestor tenha atestado que são eficazes, a AECI poderá, a seu critério, solicitar informações e documentos, a fim de realizar testes adicionais que evidenciem a eficácia do controle. O registro do teste deve observar o documento contido no Anexo IV – Formulário para Registro de Testes.

Os testes visam verificar:

- se o controle previne ou detecta falhas e fraudes;
- se o controle está funcionando conforme seu objetivo (desenho);
- se o controle é executado pela pessoa que detém a autoridade necessária.

Os testes podem variar de acordo com o nível de conforto e segurança desejados, podendo compreender: indagação, observação, exame e reexecução.

Os testes podem avaliar o desenho e a efetividade operacional dos controles, ou seja, se os controles impedem ou detectam a ocorrência de falhas nas atividades e se eles estão funcionando da forma estabelecida.

Um dos métodos de aplicação do teste de desenho é denominado *walkthrough*, que pode ser traduzido como passo a passo. Podemos entender ainda como andar ou percorrer o processo. Nesta técnica, o avaliador acompanha uma transação desde sua origem através dos processos da empresa usando os mesmos documentos e tecnologia da informação que o executor usa. Os procedimentos passo a passo geralmente incluem uma combinação de inquérito, observação, inspeção de documentação relevante e reexecução de controles[4]. Esse método pode ser aplicado para:

- Confirmar o entendimento sobre o fluxo de atividades da transação;
- Confirmar a existência de riscos e controles não identificados previamente;
- Confirmar o entendimento sobre o desenho do controle identificado;
- Avaliar a efetividade do desenho dos controles;

[4] Fonte: Adaptado de PCAOB: Public Company Accounting Oversight Board - Auditing Standard No. 5, tradução livre

- Confirmar se o controle está em operação.

Ao realizar um passo a passo nos pontos em que ocorrem procedimentos importantes, o avaliador questiona o executor sobre sua compreensão do que é exigido pelos procedimentos e controles prescritos pela empresa. Essas perguntas, combinadas com os outros procedimentos passo a passo, permitem que o avaliador obtenha uma compreensão do processo e seja capaz de identificar pontos importantes nos quais um controle necessário está ausente ou não foi projetado de forma eficaz.[3]

O *walkthrough* tem as seguintes etapas:

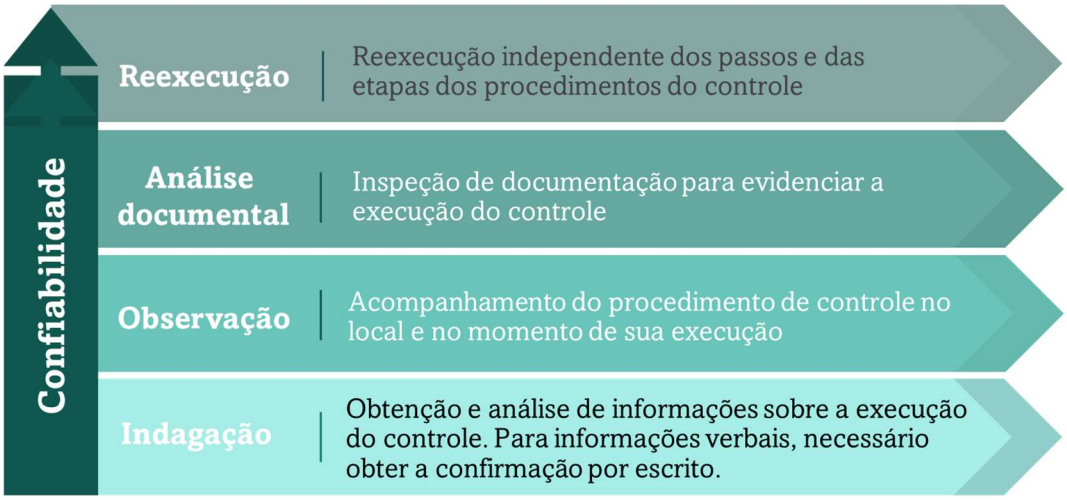
- entrevistas com os responsáveis pela transação selecionada;
- observação da realização da transação;
- análise da documentação produzida durante a execução;
- obtenção de evidências (impressão de telas contendo as travas/opções de sistemas, observação de segregação de funções, trilhas de dupla conferência, arquivos, etc); e
- registro do trabalho.

Na impossibilidade de acompanhamento de alguma etapa do *walkthrough* em tempo real, pode ser simulada a execução a partir de transação já existente.

Deficiências podem ser identificadas a partir da realização do *walkthrough*, situação em que pode ser dispensada a realização de outros testes.

Para a escolha dos testes de controle deverão ser consideradas as características do controle, o resultado da avaliação realizada pela área gestora e os riscos identificados no processo, devendo ser escolhida a técnica que traga maior conforto sobre a adequação do controle, observada a relação custo x benefício.

Figura 03 – Testes de Controles



Fonte: Adaptado do Manual de Orientações técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo Federal do CGU – 2017

- **Indagação:** trata-se de uma entrevista sobre os controles. Geralmente a indagação não oferece evidências suficientes para assegurar se um controle específico está funcionando eficazmente. Costuma ser preciso obter análise adicional, confirmando a indagação com terceiros ou examinando relatórios, manuais ou outros documentos utilizados ou gerados pela execução do

controle.

- **Observação:** não havendo documentação sobre o funcionamento de um controle, por exemplo, segregação de funções, a observação é uma forma de obtenção de evidências. Apesar de ser melhor do que a indagação, deve-se considerar que o controle pode não ser aplicado quando não estamos observando.
- **Análise documental:** utilizado para determinar se os controles manuais, como conferir e monitorar, por exemplo, são executados. Evidências podem incluir explicações por escrito, verificações assinaladas ou outras indicações de monitoramento documentadas.
- **Reexecução:** por ser o método mais oneroso, a reexecução deve ocorrer quando a indagação, a observação ou o exame das evidências não oferecem segurança suficiente de que o controle está funcionando eficazmente.

Em algumas circunstâncias, para controles automatizados, testar uma operação isolada pode ser suficiente para obter um nível elevado de conforto em relação ao funcionamento eficaz desse controle. No entanto, deve-se considerar que existem vários atributos dentro de um controle automatizado.

Encontra-se no Anexo III o formulário padrão para o registro dos testes realizados.

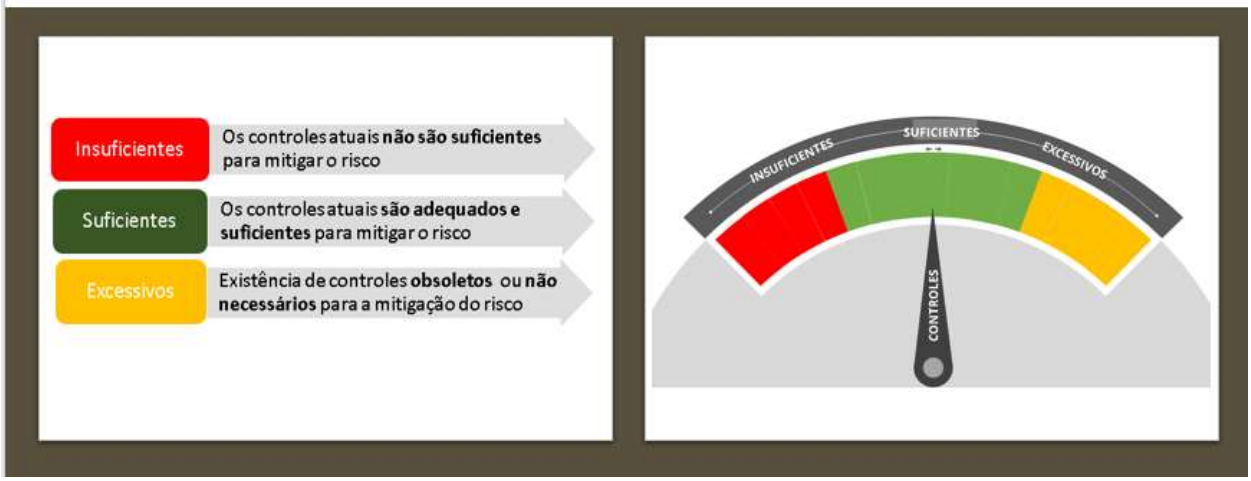
A partir do resultado dos testes, podem ser identificadas situações que representem falhas ou fragilidades no controle avaliado. Estas situações devem ser classificadas e reportadas ao gestor do processo, conforme abaixo:

- Deficiência: compreende uma ou mais falhas/fragilidades apresentadas nos testes realizados, não mitigando o fator de risco identificado. A deficiência se caracteriza pela insuficiência ou inexistência de controle, que pode levar à ocorrência do risco.
- Oportunidade de melhoria: quando é detectada uma oportunidade de ganho de eficácia para o controle ou para o processo, mas que se não for implementada, não representa fragilidade para o processo.

Efetividade dos controles

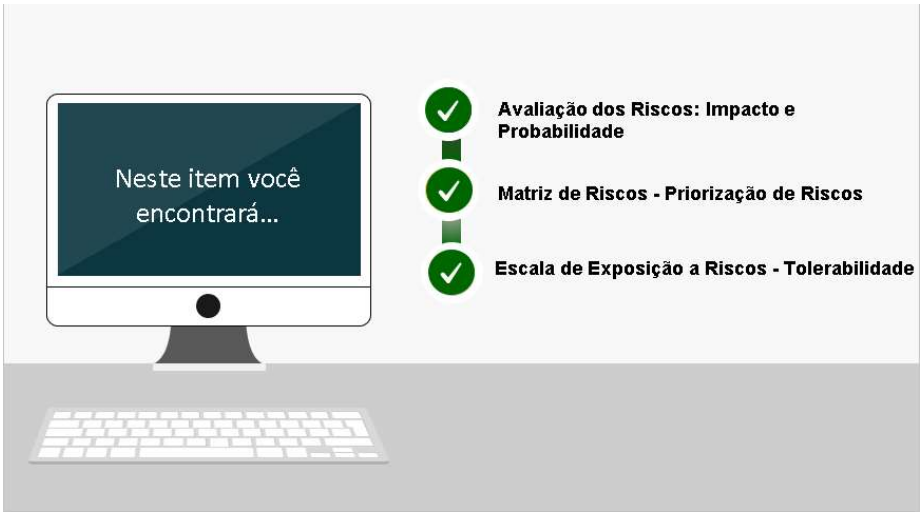
Após a avaliação individual de cada um dos controles existentes é realizada a análise coletiva, a fim de verificar o quanto o conjunto de controles existentes está adequado ao risco identificado, de acordo com os conceitos a seguir:

Figura 04 – Efetividade dos controles



Esta avaliação coletiva dos controles proporciona um direcionamento que permite ao gestor maior clareza quanto à tomada de decisão com relação à necessidade de implementação de novos controles ou melhoria de controles existentes (insuficientes), eliminação de controles ineficientes ou obsoletos (excessivos) ou ainda, evidenciar que os riscos e controles estão balanceados e adequados (suficientes).

III. Avaliação dos riscos



A etapa de avaliação dos riscos visa promover o entendimento do nível do risco, especialmente quanto à estimação da probabilidade de sua ocorrência e do impacto das consequências desses eventos, fornecendo assim uma ferramenta indicativa de quais riscos necessitam ser priorizados.

O nível do risco deve ser comparado com a escala de exposição a riscos do MCID, que determina a tolerabilidade em relação ao tipo de tratamento a ser dado.

Iniciamos a avaliação do risco, mediante os conceitos a seguir:

- **Probabilidade:** rara, pouco provável, provável, muito provável, e praticamente certa; e
- **Impacto:** muito baixo, baixo, médio, alto, e muito alto.

Probabilidade: avaliação qualitativa ou quantitativa que utiliza as experiências vivenciadas dos partícipes no processo com base em dados de eventos de riscos já materializados, dados estatísticos, ou a média histórica disponível, considerando determinado período de tempo.

A avaliação da probabilidade é realizada utilizando-se a relação de aspecto avaliativo, de acordo com o Quadro 07:

Quadro 07: Avaliação da Probabilidade

Faixa	Aspecto avaliativo
Rara	Evento que pode ocorrer apenas em circunstâncias excepcionais. Não há histórico conhecido sobre sua ocorrência ou indícios de que irá ocorrer
Pouco Provável	Evento pode ocorrer em algum momento, porém com pouca possibilidade
Provável	Evento repete-se com frequência razoável ou existem indícios de que possa ocorrer
Muito Provável	Evento deve ocorrer na maioria das circunstâncias
Praticamente Certa	Evento com altíssima probabilidade de ocorrência

Impacto: avalia-se o impacto considerando quais serão as consequências no alcance dos objetivos, caso o risco venha a ocorrer. Ele é classificado em uma das faixas do Quadro 08, considerando o descritivo do aspecto avaliativo.

Quadro 08: Avaliação do Impacto

Faixa	Aspecto avaliativo
Muito baixo	Mínimo impacto nos objetivos do processo/projeto, nas políticas setoriais e na imagem do Ministério. Não acarreta nenhuma ação dos órgãos de controle interno e externo.
Baixo	Pequeno impacto nos objetivos do processo/projeto e nas políticas setoriais. O impacto na imagem tende a limitar-se às partes envolvidas. Pode acarretar ações de caráter orientativo dos órgãos de controle interno e externo.
Médio	Moderado impacto nos objetivos do processo/projeto e nas políticas públicas, porém recuperável. Pode acarretar ações de caráter corretivo dos órgãos de controle interno e externo, inclusive com exposição na mídia por curto período de tempo.
Alto	Significativo impacto nos objetivos do processo/projeto e nas políticas públicas, de difícil reversão. Pode levar a multas e danos ao erário, com exposição significativa na mídia.
Muito alto	Catastrófico impacto nos objetivos do processo/projeto, nas políticas públicas e, até mesmo, nos objetivos estratégicos e na missão do MCID, de forma irreversível. Há possibilidade, ainda, de acarretar interrupção das atividades, com exposição na mídia nacional e internacional.

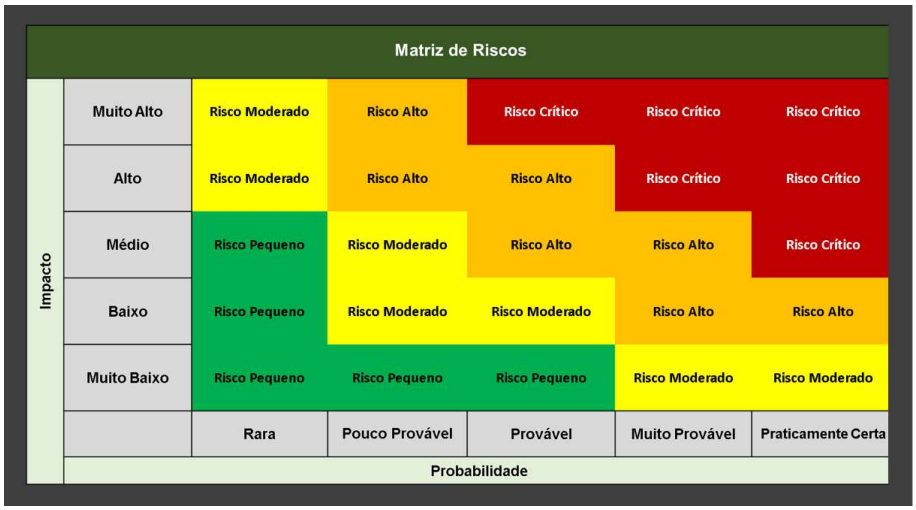
Matriz de Riscos

A matriz de riscos possibilita identificar quais os riscos que devem receber mais atenção, auxiliando o gestor na priorização quanto aos recursos que serão destinados para monitoramento, melhoria e/ou implementação de controles.

A conjunção da avaliação de probabilidade e impacto para cada risco identificado resulta em um dos 4 níveis de risco, conforme a Figura 05 – Matriz de Riscos, podendo ser:

- **Nível do Risco:** Risco Pequeno, Risco Moderado, Risco Alto e Risco Crítico.

Figura 05 - Matriz de Riscos



Escala de Exposição a Riscos - Tolerância

A exposição a riscos representa a tolerância do MCID com relação aos riscos, dispostas em 4 níveis, conforme demonstrado no Quadro 09.

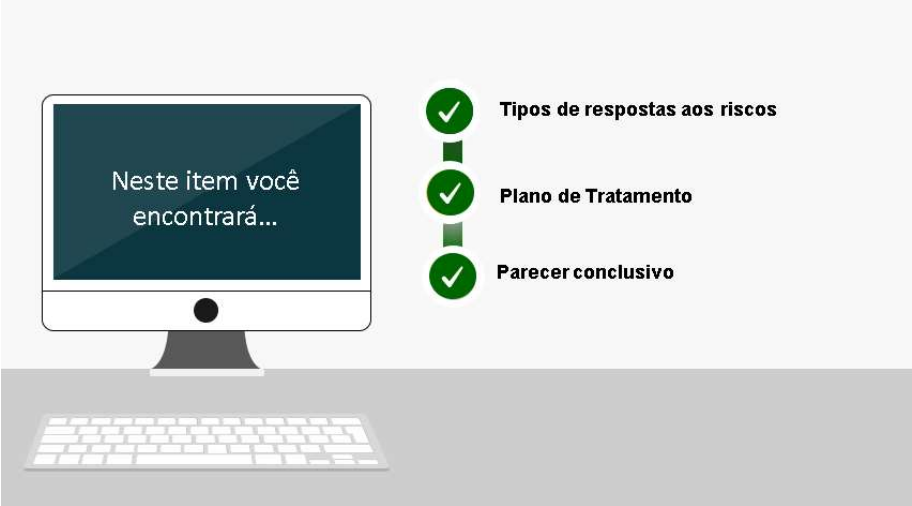
Quadro 09 - Escala de Exposição a Riscos

EXPOSIÇÃO A RISCOS	
NÍVEL DE RISCO	CRITÉRIOS PARA PRIORIZAÇÃO E TRATAMENTO DE RISCOS
Risco Crítico	Nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser comunicado à autoridade máxima da unidade e ao Cigov e ter uma resposta imediata
Risco Alto	Nível de risco além do apetite a risco. Qualquer risco nesse nível deve ser comunicado à autoridade máxima da unidade e ter um plano de tratamento para mitigação
Risco Moderado	Nível de risco dentro do apetite a risco. Não há obrigatoriedade de medidas adicionais, porém requer atividades de monitoramento específicas e atenção da gerência para que o risco não aumente. Pode-se reduzi-lo com implementações de baixo custo
Risco Pequeno	Nível de risco dentro do apetite a risco. É possível conviver com o risco mantendo as práticas e procedimentos existentes.
Obs.: A depender da situação, a autoridade máxima poderá não adotar uma resposta imediata, apresentando a devida justificativa	

Assim, para os níveis de risco Crítico e Alto, a resposta deverá sempre ser evitar, reduzir ou compartilhar. Para os níveis de risco Moderado e Pequeno, de maneira geral, pode-se aceitar. Entretanto, a depender da situação, a unidade poderá decidir por outra resposta que não sejam essas, sempre considerando o custo-benefício da implementação. Para esses casos, deverá ser apresentada justificativa.

Dessa forma, a escala de exposição a riscos fornece diretriz quanto à tolerabilidade do MCID em relação ao nível do risco, auxiliando o gestor na tomada de decisão quanto ao tipo de resposta a ser tomada.

IV. Resposta aos Riscos



A resposta aos riscos é a etapa em que, com base na análise do risco em relação aos controles existentes, poderá ser elaborada e proposta uma ou mais medidas para sua mitigação, na forma de Plano de Tratamento.

Tipos de Respostas

Há 4 possíveis tipos de respostas quanto aos riscos identificados. As respostas deverão observar os limites de exposição a riscos definidos pelo Ministério das Cidades, conforme Quadro 10:

Quadro 10 – Tipos de Respostas

Evitar	Não iniciar, ou descontinuar a atividade que origina o risco
Aceitar	Deixar a atividade como está, não adotando qualquer medida
Reduzir	Desenvolver ações para mitigar o risco, ou seja, remover suas fontes, ou reduzir a probabilidade e/ou o impacto do risco
Compartilhar	Distribuir parte do risco para outros atores (terceiros)

Plano de Tratamento

Compreende a proposição e a realização de ações para modificar o nível do risco. O nível do risco pode ser modificado por meio de medidas que reduzam, compartilhem ou evitem esses riscos.

A elaboração de um plano de tratamento deve observar as causas identificadas, de forma que, quando implementado, este tenha a propriedade de mitigação do risco e de suas consequências.

Deve-se atentar ainda que Riscos Críticos e Riscos Altos estão além do limite de exposição determinado pelo MCID. Portanto, para estes casos, o plano de tratamento é mandatório. Caso contrário, deverá ser registrada a justificativa e comunicado ao Cigov.

Os planos de tratamento serão monitorados por meio do e-Aud, cabendo aos gestores (propositores

dos tratamentos), o acompanhamento e registro de seu desenvolvimento e conclusão, juntamente com as respectivas evidências que comprovem sua implementação. A AECI realizará o registro e monitoramento dos planos, realizando uma avaliação quando da conclusão pela área gestora.

O plano de tratamento deve conter:

- Controle Proposto;
- Objetivo do Controle;
- Tipo de Controle;
- Como será implementado;
- Área responsável;
- Responsável;
- Data de início;
- Data de Conclusão.

Parecer conclusivo sobre o processo/projeto/iniciativa

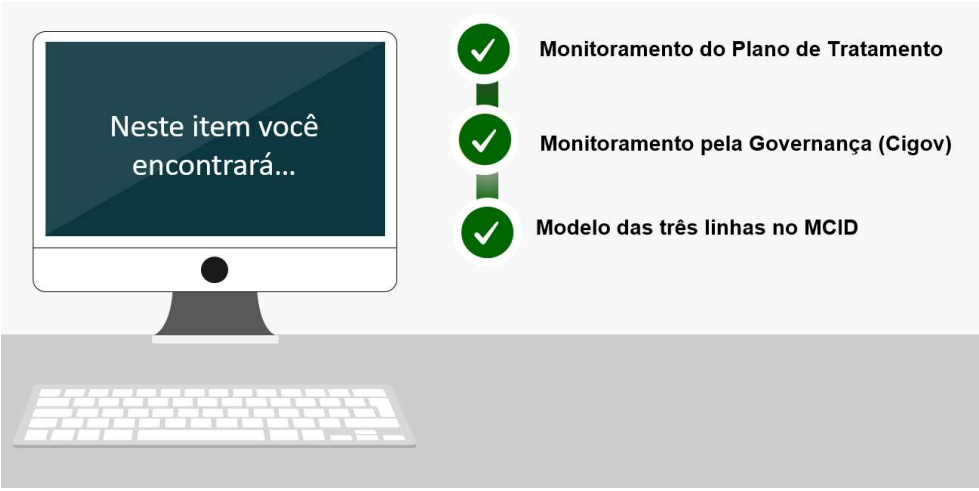
Considerando toda a avaliação, a AECI deve emitir uma conclusão final, que representa o nível de maturidade no gerenciamento de riscos e controles do objeto avaliado. Esta conclusão deve manter coerência com os riscos que possam impactar o atingimento dos objetivos e controles avaliados no trabalho, de forma a justificar o conceito escolhido, disposto no Quadro 11:

Quadro 11 – Nível de Maturidade

Nível de Maturidade – Riscos e Controles

Conceito	Descritivo
Melhores Práticas	Riscos e Controles gerenciados com eficácia, de acordo com os normativos e padrões técnicos.
Avançado	Riscos e Controles gerenciados adequadamente, entretanto foram identificadas oportunidades de melhorias e/ou pontos de atenção.
Intermediário	Riscos e Controles cujo gerenciamento necessita de melhorias pontuais.
Básico	Riscos e Controles cujo gerenciamento necessita de melhorias significativas.
Inadequado	Riscos e Controles não gerenciados, necessita de implementação de mecanismos de gestão de riscos e controles.

V. Monitoramento e Comunicação



A gestão de riscos e controles representa um importante instrumento para a gestão do órgão, governança pública e integridade, destinada a prover as melhores condições para que os objetivos organizacionais e estratégicos sejam alcançados com eficácia e eficiência, demandando dos gestores e servidores públicos a avaliação e monitoramento constantes, a fim de obter, de forma tempestiva, os resultados alcançados e as melhorias implementadas.

A fase de monitoramento é a etapa contínua em que as instâncias envolvidas com gestão de riscos interagem. Abrange a coleta e a disseminação de informações e iniciativas, a fim de assegurar a compreensão suficiente a todos os agentes envolvidos a respeito dos riscos existentes em cada decisão.

Conforme estabelecido pela Política de Gestão de Riscos e Controles Internos, cada nível do sistema de gestão de riscos do MCID possui atribuições relevantes que, apoiadas na estrutura das 3 linhas, auxiliam os agentes públicos no monitoramento dos riscos e dos controles definidos. O Anexo V – Modelo das Três Linhas (IIA) descreve mais informações a respeito das principais funções e suas relações entre essas linhas.

Figura 06 – Sistema de Gestão de Riscos e Controles Internos

Conforme Figura 06, o Sistema de Gestão de Riscos e Controles Internos contém os níveis estratégico, tático e operacional. As unidades organizacionais e os gestores de risco (1ª linha) são os responsáveis primários para que os riscos e controles permaneçam a níveis considerados adequados. Além disto, cabe

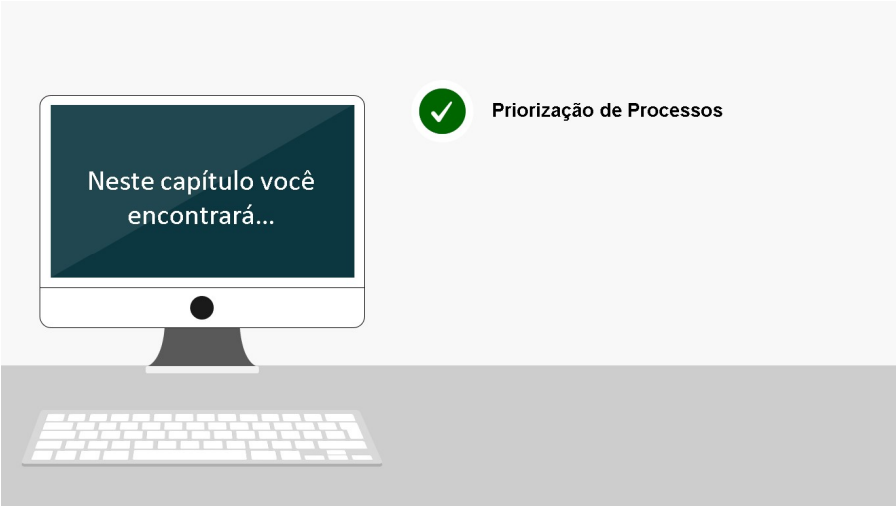
o monitoramento das ações propostas para tratamento dos riscos, de forma a prover sua implementação e registro. As áreas gestoras são responsáveis também por comunicar e fornecer informações sobre a gestão de riscos e controles para a AECI (2ª linha), sempre que solicitado.

A AECI, como 2ª linha, é responsável pelo monitoramento sobre a gestão de riscos e controles do MCID e por acompanhar os planos de tratamento elaborados pelos gestores, de forma a zelar para que as ações propostas sejam concluídas pelos proponentes, bem como, realizar o reporte para a governança, sempre que necessário.

O Cigov, por sua vez, é a instância da governança do MCID responsável pelo sistema de gestão de riscos e controles internos, exercendo o monitoramento dos riscos e controles por meio dos reportes realizados, além de outras atribuições.

A CGU representa a 3ª linha e realiza seu papel de forma totalmente independente, com o propósito de contribuir para o aprimoramento das políticas públicas e a atuação das organizações.

CAP. 03 – Priorização de Processos



Os Critérios de Priorização de Processos (CPP) objetivam estabelecer a identificação de processos, projetos ou iniciativas prioritárias de uma Unidade para fins de gerenciamento de riscos e controles, de forma participativa com as secretarias finalísticas.

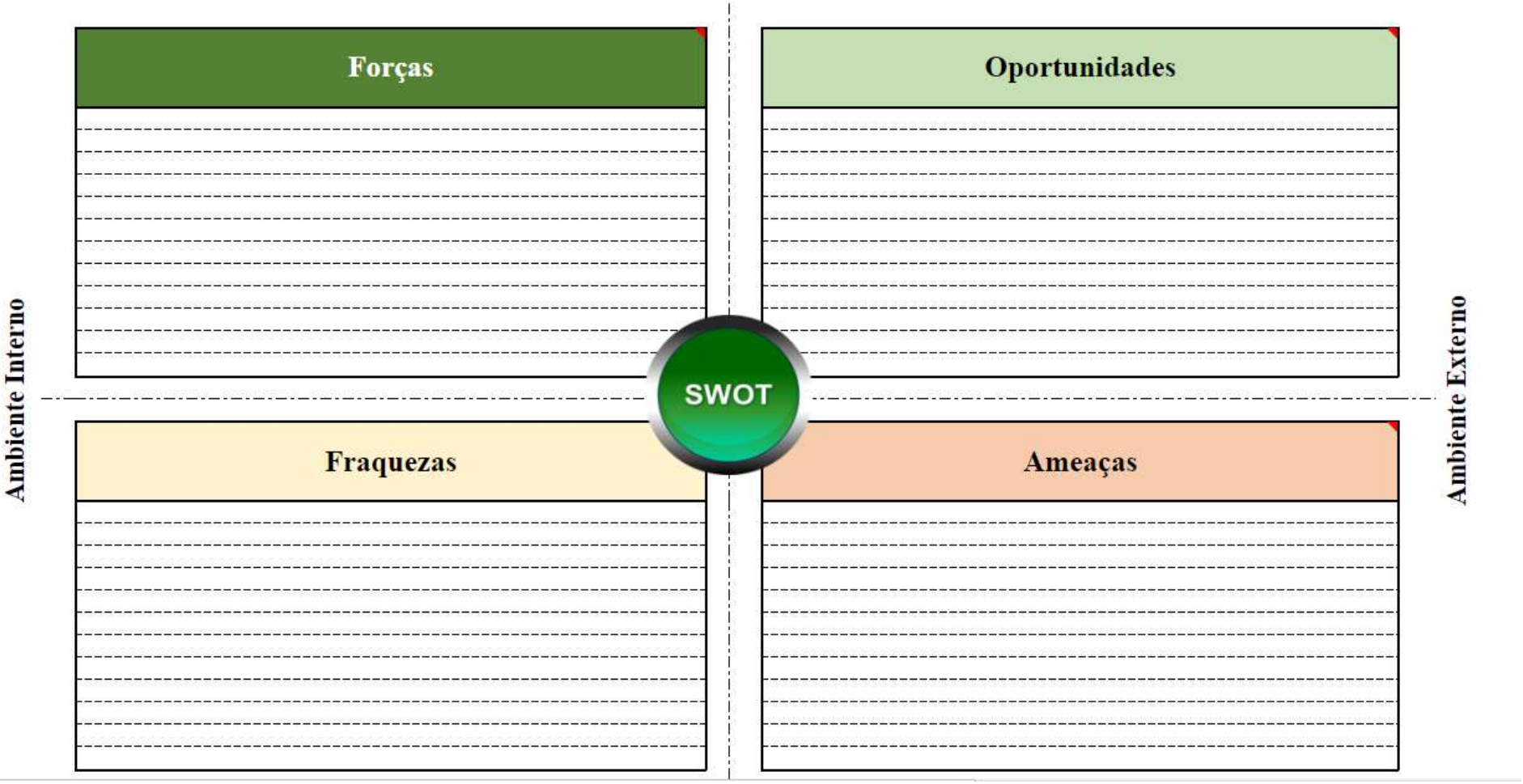
São considerados critérios qualitativos e quantitativos para classificar os processos, projetos ou iniciativas em função do seu grau de exposição, de acordo com os seguintes conceitos:

- Essencial: expressa os processos mais significativos, que deverão ter prioridade sobre os demais no gerenciamento de riscos;
- Relevante: expressa os processos de grande importância ou que merecem destaque, e que deverão ter uma prioridade média sobre os demais no gerenciamento de riscos;
- Moderado: expressa os processos de menor importância, que deverão ter prioridade baixa sobre os demais no gerenciamento de riscos.

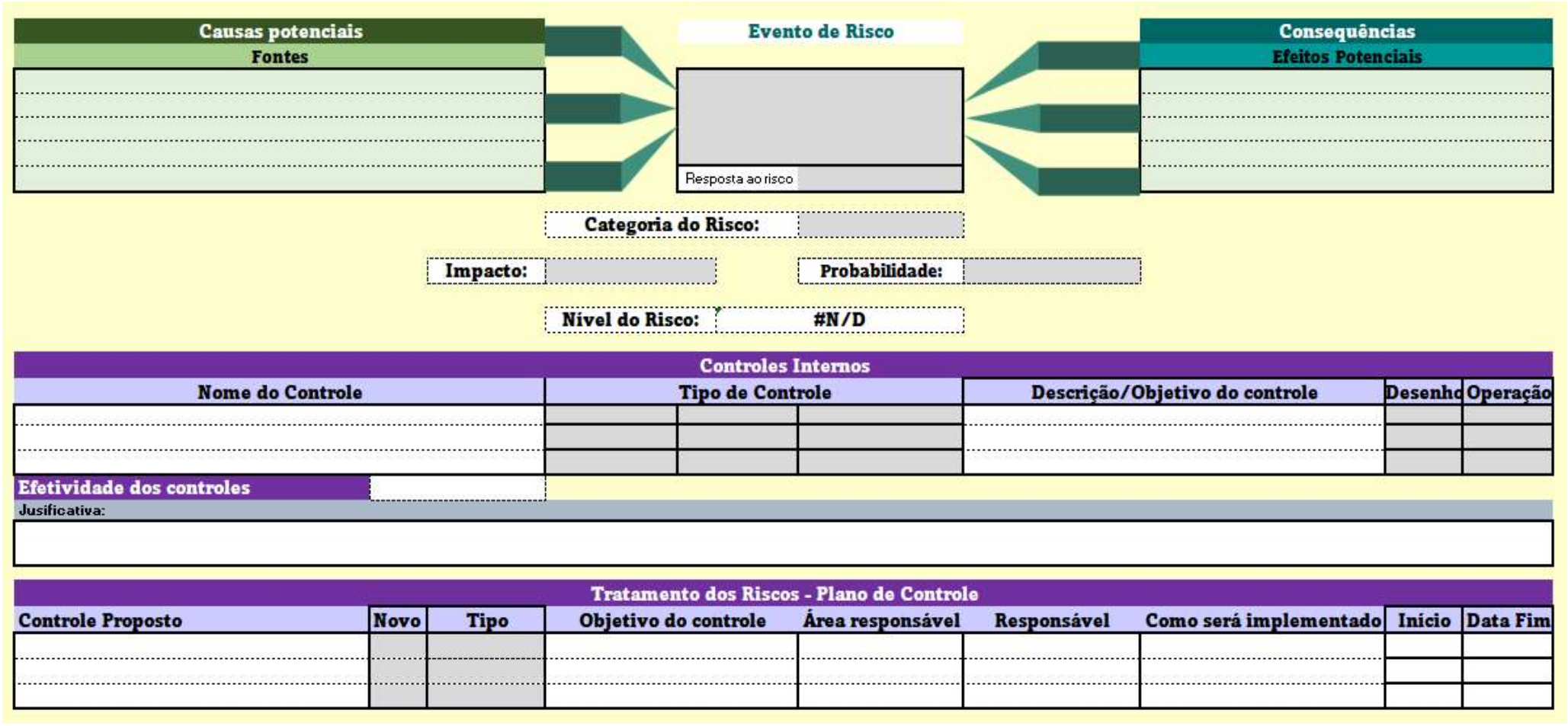
Os critérios observam a cadeia de valor do Planejamento Estratégico Institucional do MCID, associada ao modelo de gestão estratégica de processos.

Anexos

Anexo I - Matriz SWOT



Anexo II – Bow Tie Adaptado



Causas potenciais	Evento de Risco	Consequências
Fontes		Efeitos Potenciais
	Resposta ao risco	

Categoria do Risco:	
Impacto:	
Probabilidade:	
Nível do Risco:	#N/D

Controles Internos

Nome do Controle	Tipo de Controle			Descrição/Objetivo do controle	Desenho	Operação

Efetividade dos controles	
Jusificativa:	

Tratamento dos Riscos - Plano de Controle

Controle Proposto	Novo	Tipo	Objetivo do controle	Área responsável	Responsável	Como será implementado	Início	Data Fim

Anexo III – Planilha para Avaliação de Dados não Estruturados (DnE)

Controle:	

Requisitos	Descrição	S/N
Controle de acesso	Planilha: Verificar se a planilha possui senha de proteção de acesso e é arquivada e utilizada em diretório de rede com controle de acesso, mediante a análise dos logs de acesso fornecidos pela área de TI Aplicativo: Verificar se o banco de dados restringe o acesso às informações mediante senha	
Controle de mudanças	Verificar se as mudanças realizadas no sistema possuem registro passível de rastreamento (LOG)	
Documentação	Verificar se os procedimentos usados para operacionalizar a planilha estão documentados	
Acurácia e integridade de dados	Verificar se são efetuadas conciliações formais dos dados de entrada e de saída (resultados), que assegurem a abrangência, a consistência, a integridade e a confiabilidade deles. Essas conciliações devem ser documentadas e realizadas por funcionário diferente daquele que utiliza a base de dados	
Validação lógica	Verificar se existe procedimento de revisão da lógica implementada na planilha por funcionário diferente daquele que a desenvolveu. Essa revisão deve ser documentada. (Ex:. cópias das mensagens de correio eletrônico com a descrição das alterações efetuadas pelo funcionário responsável e a confirmação da validação dessas alterações por outro funcionário)	
Proteção lógica	Averiguar se foi implementada a proteção de células sensíveis da planilha, como as que contêm dados principais para o processamento e fórmulas	

Anexo IV – Formulário para registro dos Testes

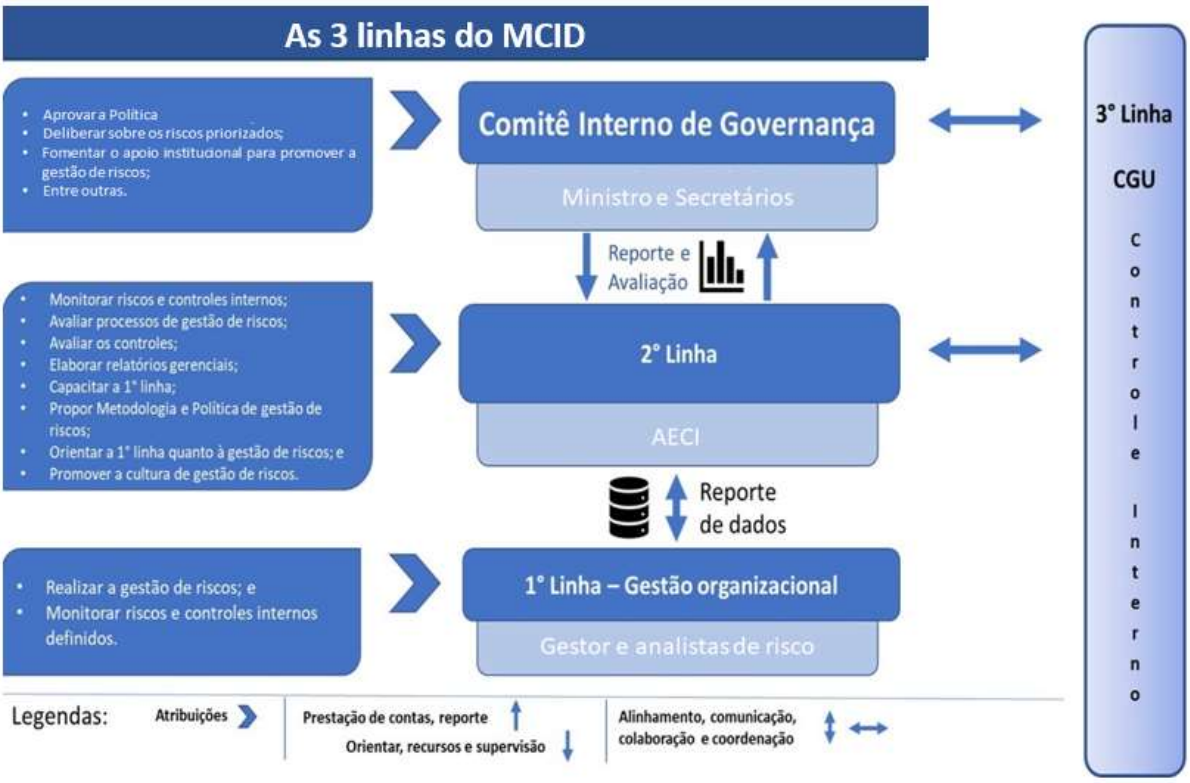
Registro de Testes em Controles

Controle	Indicar o controle a ser testado
Natureza do Teste	Indagação/Observação/Exame/Reexecução
Objetivo do teste	O que se pretende testar ou comprovar com a realização do teste
Insumos	Descrever os insumos que serão utilizados para a realização do teste
Período	Período considerado para os testes de operacionalização
Extensão	População/Amostra/Outro critério
Critério de seleção	Critério de seleção do objeto a ser testado
Procedimentos	Indicar como será realizado o teste, o que será verificado e de que forma
Resultado	Com exceção ou sem exceção
Análise	Breve relato sobre a execução e resultado do teste

Anexo V – Modelo das Três Linhas (IIA)

No âmbito do MCID, a referida estrutura é apresentada da seguinte forma, conforme Figura 7:

Figura 7: As 3 Linhas no MCID



Anexo VI - Matriz RACI

Legenda	
A - Aprovador	É quem aprova ou valida formalmente a atividade ou o produto dela resultante.
P - Promotor	É quem promove ou fomenta a execução da atividade.
R - Responsável	É quem executa a atividade formalmente.
C - Consultado	É quem gera uma informação que agrega valor para a execução de uma atividade ou quem apoia sua execução.
I - Informado	É quem precisa ser notificado do resultado da atividade.

Matriz de Responsabilidades													
Instâncias de Supervisão							Atribuições	Periodicidade					
Nível Estratégico		Nível Tático		Nível Operacional									
Ministro de Estado	Cigov	Secretaria Executiva	AECI	Unidades Organizacionais	Gestores de Riscos	Analistas de Riscos		Mensal	Quadrimestral	Semestral	Anual	Quando necessário	Sempre
I	A	C	R	C	C	C	Revisão da Política de Gestão de Riscos.					X	
I	I	C	R	C	C	C	Revisão da Metodologia de Gestão de Riscos.					X	
I	A	C	R	I	I	I	Definição do apetite a risco do Ministério.					X	
I	A	C	R	C	C	C	Selecionar os processos/projetos cujos riscos serão gerenciados				X		
I	I	I	P/ I	I	A	R	Identificar e avaliar os riscos dos processos selecionados.						X
I	I	I	I	R	I	I	Indicar os Gestores de Risco.					X	
I	I	I	P/ R	C	R	C	Monitorar o cumprimento dos planos de tratamento definidos.						X
I	A	I	R	C	C	C	Elaboração de relatório sobre riscos críticos e altos e a efetividade das medidas de controle implementadas.				X		

Matriz de Responsabilidades													
				Instâncias de Supervisão			Atribuições	Periodicidade					
Nível Estratégico		Nível Tático		Nível Operacional									
Ministro de Estado	Cigov	Secretaria Executiva	AECI	Unidades Organizacionais	Gestores de Riscos	Analistas de Riscos		Mensal	Quadrimestral	Semestral	Anual	Quando necessário	Sempre
I	I	I	P/ R	C	R	C	Monitoramento do risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados, e a efetividade dos controles implementados.						X
I	I	I	P/ R	C	C	C	Monitorar o desempenho do Sistema de Gestão de Riscos e sua eficácia em relação aos objetivos pretendidos.						X
I	I	I	P/ R	C	C	C	Orientar as unidades organizacionais na aplicação da Metodologia de Gestão de Riscos.						X
I	I	I	P/ R	C	C	C	Estimular a contínua capacitação do corpo funcional em gestão de riscos e em outras competências técnicas correlatas, por meio de palestras, cursos e eventos.						X
R	R	R	P	I	I	I	Fomentar o apoio institucional para promover a gestão de riscos, em especial os seus recursos, o relacionamento entre as partes interessadas e o desenvolvimento contínuo dos servidores.						X

Matriz de Responsabilidades												
				Instâncias de Supervisão			Atribuições e Interelacionamentos	Periodicidade				
Nível Estratégico		Nível Tático		Nível Operacional								
Ministro de Estado	Cigov	Secretaria Executiva	AECI	Unidades Organizacionais	Gestores de Riscos	Analistas de Riscos		Mensal	Quadrimestral	Semestral	Quando necessário	Sempre
R	R	R	P	R	R	R	Garantir o alinhamento da gestão de riscos aos padrões de ética e de conduta, em conformidade com o Programa de Integridade do MCID.					X
P	P	P	R/P	I/C	I/C	I/C	Promover inovação e adoção de boas práticas de governança, integridade, riscos e controles internos da gestão.					X
R	R	R	C	I	I	I	Institucionalização de estruturas adequadas de governança, de gestão da integridade, riscos e controles internos.					X
I	A	P	P/R	C/I	I	I	Políticas, diretrizes, metodologias e mecanismos de monitoramento e comunicação para a gestão de integridade, riscos e controles internos.					X
I	A	P	P/R/I	R/I	R/I	I	Ações para disseminação da cultura de gestão de integridade, riscos e controles internos.					X
I	A	I	P/R	C/I	C/I	C/I	Método de priorização de processos/projetos para a gestão de integridade, riscos e controles internos.				X	
R	R	R	P	C/I	C/I	C/I	Recomendações e orientações para o aprimoramento da gestão de integridade, riscos e controles internos.				X	
I	I	I	R	C/I	C/I	C/I	Disponibilidade de informações adequadas sobre gestão de integridade, riscos, e controles internos em todos os níveis, no âmbito das unidades.					X

Referências Bibliográficas

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO 31000. Gestão de Riscos: Princípios e Diretrizes. Rio de Janeiro. 2018.

- Banco Central do Brasil. Resolução nº 4.557, de 23 de fevereiro de 2017 - Estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital.

- BRASIL. Controladoria-Geral da União e extinto Ministério do Planejamento, Desenvolvimento e Gestão. Instrução Normativa Conjunta nº 1, Brasília, 10 de maio de 2016.

- BRASIL. Decreto nº 9203, de 22 de novembro de 2017. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/D9203.htm.

- BRASIL. Ministério da Economia. Guia de Gestão de Riscos do Ministério da Economia, Versão 2, Brasília. 2021. Disponível em: file:///D:/Downloads/Guia%20Gest%C3%A3o%20de%20Riscos%20V%20FINAL%2031.05%20(1).pdf.

- BRASIL. Ministério da Economia. Resolução Comitê de Gestão de Riscos, Transparência, Controle e Integridade do Ministério da Economia - CRTCI nº 2, de 2019, Política de Gestão de Riscos do ME. 2019.

- BRASIL. Ministério do Desenvolvimento Regional. Resolução CIGOV nº 1, de 23 de março de 2022. Aprova a Política e a Metodologia de Gestão de Riscos do Ministério do Desenvolvimento Regional.

- BRASIL. Ministério do Desenvolvimento Regional. Plano Estratégico Institucional MDR. Disponível em: https://www.gov.br/mdr/pt-br/acesso-a-informacao/institucional/planejamento-estrategico-institucional/SumrioExecutivoPlanoEstratgicoMDRDez.2021.v2.pdf.

- BRASIL. Ministério do Planejamento, Orçamento e Gestão. 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. Disponível em: https://www.in.gov.br/materia/-asset_publisher/Kujrw0TZC2Mb/content/id/21519355/do1-2016-05-11-instrucao-normativa-conjunta-n-1-de-10-de-maio-de-2016-21519197.

- BRASIL. Tribunal de Contas da União. Manual de Gestão de Riscos do TCU – Um passo para a eficiência - 2 edição. Brasília. 2020.Disponível em: https://portal.tcu.gov.br/planejamento-governanca-e-gestao/gestao-de-riscos/manual-de-gestao-de-riscos/.

- Instituto de Auditores Internos do Brasil (IIA). Modelo das Três Linhas do IIA: Uma atualização das Três Linhas de Defesa, Versão 2, 2020. Disponível em: https://iiabrasil.org.br/noticia/novo-modelo-das-tres-linhas-do-iia-2020.

- Public Company Accounting Oversight Board - PCAOB: - Auditing Standard No. 5. 2016. Disponível em: https://pcaobus.org/oversight/standards/archived-standards/pre-reorganized-auditing-standards-interpretations/details/Auditing_Standard_5.

– The Committee of Sponsoring Organizations of the Treadway Commission – COSO. Enterprise Risk Management - Integrating with Strategy and Performance. COSO. 2017.