METODOLOGIA DE AVALIAÇÃO DE RISCOS E CONTROLES INTERNOS

MINISTÉRIO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL

GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Guia Rápido

AECI - Assessoria Especial de Controle Interno

Sumário

CAP. 01 – Introdução 1
CAP. 02 – Avaliação de Riscos e Controles Internos 1
Etapa 1 – Análise de Ambiente e dos Objetivos 1
Definição do Escopo do Trabalho 1
Insumos 1
Análise do Ambiente e dos Objetivos 1
Etapa 2- Identificação dos Riscos 2
Identificar e descrever os eventos de riscos, suas causas e consequências 2
Categorias dos riscos 2
Técnica Bow Tie 3
Controles 3
Avaliação dos controles 4
Testes nos controles 5
Efetividade dos controles 5
Etapa 3 - Avaliação dos riscos 6
Impacto e Probabilidade 6
Matriz de Riscos - Priorização de Riscos 6
Escala de Exposição a Riscos 7
Etapa 4 - Resposta aos Riscos 7
Tipos de Respostas 7
Plano de Tratamento 8
Parecer conclusivo sobre o processo/projeto/iniciativa 8
Etapa 5 - Monitoramento e Comunicação 8
CAP. 03 – Priorização de Processos 9
ANEXOS 10
Anexo I - Matriz SWOT 11
Anexo II – Bow Tie Adaptado 12

CAP. 01 – Introdução

Este Guia Rápido é direcionado aos gestores quando da avaliação de riscos e controles. Ele traz uma síntese da Metodologia de Avaliação de Riscos e Controles Internos.

A Metodologia tem foco na contribuição que uma gestão eficiente de riscos e controles internos fornece para o alcance dos objetivos propostos por meio da identificação e tratamento dos riscos mais relevantes e na identificação de 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.

Abrangência: Ministério da Integração e do Desenvolvimento Regional, com indicação de utilização por todas as unidades, de forma a promover uma linguagem única de riscos e controles.

Etapas para a avaliação de riscos e controles:

Registro da avaliação:

Sistema Agatha - https://agatha.mdr.gov.br/#

Monitoramento dos controles propostos no Plano de Tratamento: quanto

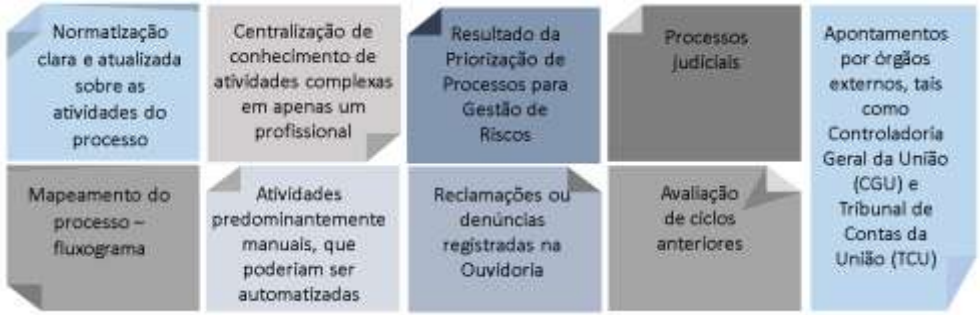
Sistema e-Aud - https:// https://eaud.cgu.gov.br/

CAP. 02 – Avaliação de Riscos e Controles Internos

Etapa 1 – Análise de Ambiente e dos Objetivos

Definição do Escopo do Trabalho: deve ser detalhado e delimitado o objeto a ser avaliado (escopo do trabalho). Por exemplo, no caso do processo, a partir de qual etapa ou atividade e até qual fase será feita a avaliação.

Insumos: os insumos, tais como os citados a seguir, podem auxiliar na compreensão do processo e deverão ser observados:



Análise do Ambiente e dos Objetivos: levantamento e registro dos aspectos externos e internos essenciais ao alcance dos objetivos, que podem influenciar a capacidade de atingir os resultados planejados.

Caso necessário, propomos a utilização da Matriz SWOT (documento disponível no Anexo I).

Etapa 2- Identificação dos Riscos

Identificar e descrever os eventos de riscos, suas causas e consequências: reconhecimento, descrição e registro dos eventos dos riscos mais relevantes, com a caracterização de suas prováveis causas e possíveis consequências. Deverá ser desenvolvida uma relação de eventos de riscos que podem comprometer os resultados e o alcance dos objetivos, que possam afetar o valor público a ser entregue à sociedade.

Perguntas que podem auxiliar na identificação dos eventos de riscos:

O que pode dar errado?	O que pode gerar perda?
O que pode nos levar à falha?	O que pode gerar retrabalho?
Quais os principais pontos de vulnerabilidade?	O que pode ocasionar dano a imagem?
Como alguém poderia fraudar ou roubar?	Existe algum impedimento legal para prosseguimento da atividade?
As informações são restritas e protegidas?	Quais gargalos podem comprometer a entrega?
As informações são automatizadas?	Existe disponibilidade de pessoas capacitadas para cuidar do assunto?
Como podemos saber se estamos alcançando nossos objetivos?	Tenho informações claras, suficientes e disponíveis para tomar decisão?
Quais atividades têm maior grau de complexidade?	Tenho disponibilidade orçamentária?
Existem atividades complexas concentradas em apenas uma pessoa?	A equipe conhece toda a legislação, manuais etc que tratam do assunto?
Onde são tomadas as decisões mais complexas e relevantes?	

Categorias dos riscos: a classificação do evento de risco deverá observar aspectos subdivididos nas seguintes categorias:

Categorias	
Operacional	Associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas. Esta definição inclui o risco legal.
Orçamentário	Podem comprometer a capacidade do Ministério de contar com os recursos orçamentários e financeiros, ou que possam comprometer a própria execução orçamentária
Imagem	Podem comprometer a confiança da sociedade em relação à capacidade do Ministério em cumprir sua missão
Conformidade	Eventos derivados de descumprimento legislativo ou normativo que podem comprometer as atividades do Ministério
Integridade	Relacionados a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer valores e padrões preconizados pelo Ministério
Estratégico	eventos que podem comprometer a estratégia do Ministério devido a mudanças 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.

Técnica Bow Tie

Como apoio à coleta estruturada de informações é utilizada a técnica de Bow Tie para a identificação do evento de risco, suas causas e consequências. Deverá ser utilizado um Bow tie para cada evento de risco identificado (arquivo disponível no Anexo II).

Controles

Identificação e avaliação dos controles: 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.

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.

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.

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, tais como Políticas, normas, Código de Ética, treinamentos. Os controles em nível de entidade auxiliam na mitigação dos riscos, no entanto, tem precisão menor do que os controles operacionais
Operacionais	Os controles operacionais ou transacionais são os controles que afetam de forma mais direta o processo

O quadro a seguir relaciona alguns 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:

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 à Natureza:

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

Uma vez os controles identificados e classificados, parte-se para a avaliação dos controles, com relação ao seu desenho e operação, de forma a verificar sua eficácia, conforme critérios definidos no quadro a seguir, que observa existência, formalização e suficiência.

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): são atividades ou controles realizados por meio de planilhas eletrônicas, sistemas, bancos de dados e outras soluções.

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, conforme o quadro a seguir:

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. O Bow Tie completo encontra-se no Anexo II deste documento.

Testes nos controles

Caso o gestor tenha atestado que os controles são eficazes, a AECI poderá, a seu critério, solicitar informações e documentos, a fim de realizar testes adicionais que evidenciem a eficácia do controle.

Caso sejam 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:

Esta avaliação coletiva dos controles proporciona um direcionamento que permite ao gestor maior clareza quanto à tomada de decisão com relação a 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).

A avaliação é registrada no Bow Tie.

Etapa 3 - Avaliação dos riscos

Impacto e Probabilidade: visa promover o entendimento do nível do risco, fornecendo assim uma ferramenta indicativa de quais riscos necessitam ser priorizados. Iniciamos a avaliação do risco, mediante os conceitos de probabilidade e impacto, conforme a seguir:

Probabilidade: avaliação qualitativa ou quantitativa que utiliza as experiências vivenciadas no processo, ou a média histórica disponível, considerando determinado período de tempo, conforme as faixas e aspectos do quadro a seguir:

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: considera quais serão as consequências no alcance dos objetivos, caso o risco venha a ocorrer, conforme as seguintes faixas e conceitos:

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 MIDR, de forma irreversível. Há possibilidade, ainda, de acarretar interrupção das atividades, com exposição na mídia nacional e internacional.

Matriz de Riscos - Priorização de Riscos**:** possibilita identificar quais os riscos que devem receber mais atenção, auxiliando na priorização quanto aos recursos que serão destinados para monitoramento, melhoria e/ou implementação de controles, podendo ser**:** Risco Pequeno, Risco Moderado, Risco

Alto e Risco Crítico.

Escala de Exposição a Riscos

A exposição a riscos representa a tolerância do MIDR com relação aos riscos, auxiliando o gestor na tomada de decisão quanto ao tipo de resposta a ser tomada.

Níveis de risco Crítico e Alto: a resposta deverá sempre ser evitar, reduzir ou compartilhar. 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.

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 CEG 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	

Etapa 4 - Resposta aos Riscos

Tipos de Respostas

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, conforme o quadro abaixo:

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

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.

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.

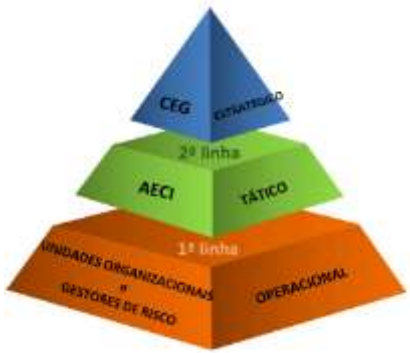
Parecer conclusivo sobre o processo/projeto/iniciativa

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:

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.

Etapa 5 - Monitoramento e Comunicação



O monitoramento é a etapa contínua em que as instâncias envolvidas com gestão de riscos interagem a fim de assegurar a compreensão suficiente a todos os agentes envolvidos a respeito dos riscos existentes em cada decisão.

Cada nível do sistema de gestão de riscos do MIDR possui atribuições relevantes que, apoiadas na estrutura das 3 linhas, auxiliam os agentes públicos no monitoramento dos riscos e dos controles definidos.

Conforme Figura, 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 e reporte sobre a gestão de riscos e controles do MIDR para a governança, por acompanhar os planos de tratamento elaborados pelos gestores, de forma a zelar para que as ações propostas sejam concluídas pelos proponentes.

O CEG, por sua vez, é a instância da governança do MIDR 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.

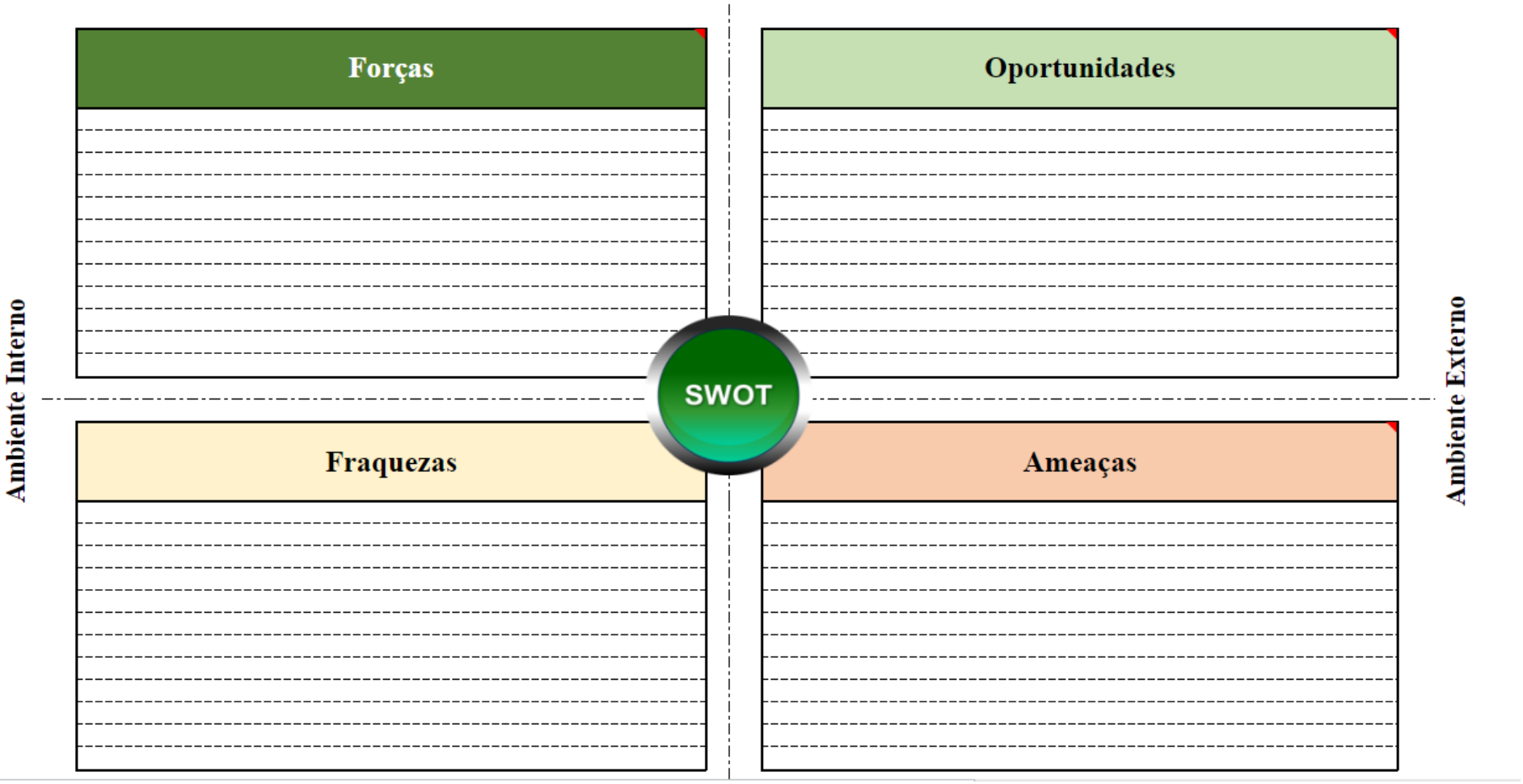
CAP. 03 – Priorização de Processos

Os critérios para a priorização de processos visam estabelecer a identificação de processos prioritários de uma Unidade para fins de gerenciamento de riscos e controles, de forma participativa com as secretarias finalísticas.

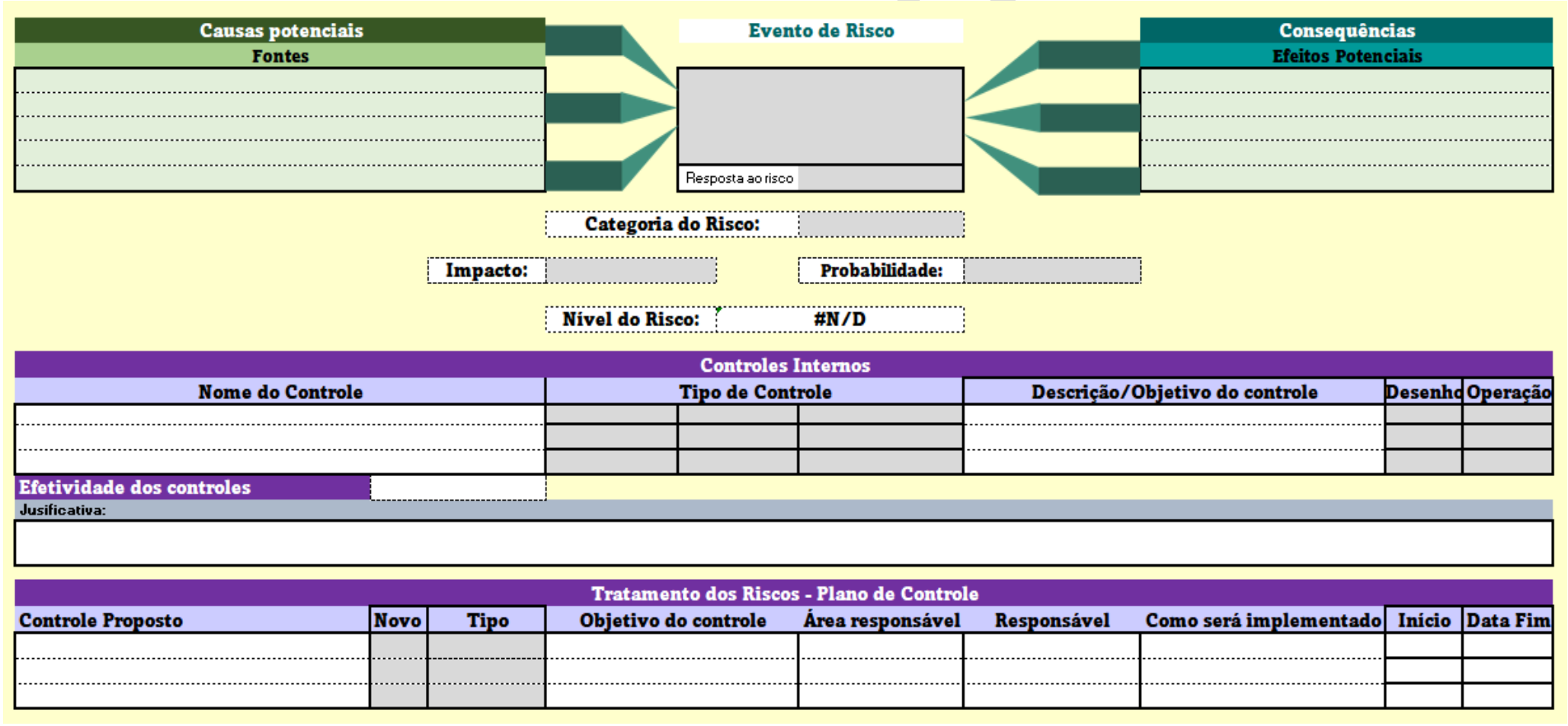
Os critérios devem observar a cadeia de valor do Planejamento Estratégico Institucional do MIDR, associada ao modelo de gestão estratégica de processos

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