Tribunal Regional Eleitoral de Rondônia

Secretaria de Tecnologia da Informação

MANUAL DO PROCESSO DE GESTÃO DE RISCOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Justiça
Eleitoral

Porto Velho - RO

Setembro de 2019

Sumário

1. Propósito do processo

Proteger e criar valor para o TRE-RO, guiando os gestores e suas equipes, na identificação, análise, registro, comunicação e tratamento de riscos que permeiam os projetos e os processos da área de Tecnologia da Informação e Comunicação.

2. Evento ou condição para início do processo

As condições que deflagram a execução do processo, sem prejuízo de outras que possam surgir, são:

- Determinação das instâncias de governança de TIC
- Achados de auditoria

3. Produtos do processo

Constituem produtos do processo:

- Plano de gestão de riscos de TIC
- Inventário de lições aprendidas
- Matriz de classificação de riscos
- Tabela do contexto organizacional da unidade de TIC
- Tabela dos critérios de riscos de TIC
- Planos de respostas aos riscos de TIC

4. Detalhamento das atividades

Processo: Estabelecimento do contexto geral
Atividade: 1. Identificar os objetos relevantes
Entradas: ✓ Plano Estratégico de TIC (PETIC) ✓ Plano tático de TIC (PDTIC)
Saídas: ✓ Relação contendo os objetos que deverão necessariamente constar no plano de gestão de riscos
Descrição da atividade: ✓ Identificar quais os objetos (processos de trabalho; projetos; iniciativas; planos de ação) mais relevantes para o alcance dos objetivos estratégicos ✓ Identificar as pessoas envolvidas nas entregas dos objetos identificados
Observações: ✓ Sem informação

Materiais auxiliares:

- ✓ Sem informação

Processo:
Estabelecimento do contexto geral

Atividade:

2. Avaliar lições aprendidas

Entradas:

- ✓ Informações coletadas em repositório de lições aprendidas (Por exemplo o SEI, Sistema de Ger. de Projetos) e/ou em entrevistas e reuniões com os gerentes de projetos e processos.
- ✓ Relação contendo os objetos identificados para a gestão de riscos

Saídas:

- ✓ Inventário de lições aprendidas extraídas do portfólio de projetos e dos processos de TIC

Descrição da atividade:

- ✓ Buscar em repositórios como SEI e Sistema de Gerenciamento de Projetos, os registros das lições aprendidas com o gerenciamento dos processos e projetos do TRE-RO
- ✓ Identificar a partir das informações registradas nos repositórios, os eventos de riscos e as lições aprendidas com esses eventos. Essas informações poderão ser coletadas também junto aos gerentes e aos envolvidos nos projetos e processos.

Observações:

- ✓ Sem informação

Materiais auxiliares:

- ✓ Sem informação

Processo:
Estabelecimento do contexto geral

Atividade:

3. Estabelecer os fatores internos e externos

Entradas:

- ✓ Inventário de lições aprendidas

Saídas:

- ✓ Tabela com a categorização de fatores de riscos internos e externos à TIC

Descrição da atividade:

- ✓ Estabelecer os fatores internos e externos à unidade de TIC, que em conjunto com os critérios de riscos, formarão o ambiente de gerenciamento de riscos de TIC.

Exemplo de tabela com categorização de fatores de riscos:

FATORES INTERNOS	FATORES EXTERNOS
CONFORMIDADE E FISCALIZAÇÃO • Normatização, controle e fiscalização interna • Gestão dos elementos que influenciam o alcance dos objetivos estratégicos	**REGULAMENTAÇÃO** • Ambiente regulatório • Aderência aos principais requisitos regulatórios externos
RECURSOS HUMANOS • Carga de trabalho • Segregação de funções •Clima organizacional	**FORNECEDORES** • Relação com os fornecedores • Sanções ao contratado • Cláusulas contratuais sobre a entrega do objeto contratado
TECNOLOGIA DA INFORMAÇÃO • Abrangência dos benefícios da TI • Demanda interna por recursos de TI • Definição de parâmetros mínimos de qualidade e eficiência dos serviços prestados pela TI • Alinhamento da TI ao plano corporativo de continuidade de negócios	**DESASTRES** • Inundação, incêndio e outros
SEGURANÇA DA INFORMAÇÃO • Controles de segurança física • Alinhamento entre os controles de segurança física e lógica • Existência do Plano de Continuidade de negócios ou Plano de Recuperação de Desastres	**REPUTAÇÃO** • Percepção da sociedade • Segurança do Processo Eleitoral
CULTURA ORGANIZACIONAL • Adaptação da cultura organizacional às mudanças no contexto interno	**AMBIENTE CULTURAL, SOCIAL E POLÍTICO** • Mudanças da alta gestão
ECONÔMICOS • Disponibilidade financeiro-orçamentária	

Observações:

- ✓ Sem informação

Materiais auxiliares:

- ✓ Sem informação

Processo:
Estabelecimento do contexto geral

Atividade:

4. Estabelecer a escala de probabilidade

Entradas:

- ✓ Inventário das lições aprendidas
- ✓ Tabela de fatores de riscos

Saídas:

- ✓ Tabela de escala de probabilidade

Descrição da atividade:

- ✓ Estabelecer a(s) Escala(s) de Probabilidade que será(ão) utilizada(s) como base para aplicação nos casos concretos

Observações:

- ✓ A seguir um exemplo da tabela de escala de probabilidade:

ESCALA DE PROBABILIDADE			
DESCRITOR	**DESCRIÇÃO**	**OCORRÊNCIAS NOS ÚLTIMOS CINCO ANOS**	**NÍVEL**
Muito Baixa	Evento extraordinário, sem histórico de ocorrência.	Nº de ocorrências = 0	1
Baixa	Evento casual e inesperado.	Nº de ocorrências <= 5	2
Média	Evento esperado, de frequência moderada, e com histórico de ocorrência parcialmente conhecido.	5 < Nº de ocorrências <=10	3
Alta	Evento usual, com histórico de ocorrência amplamente conhecido.	10 < Nº de ocorrências <= 15	4
Muito Alta	Evento repetitivo e constante.	Nº de ocorrências > 15	5

Materiais auxiliares:

- ✓ Sem informação

Processo:
Estabelecimento do contexto geral

Atividade:

5. Estabelecer a escala de impacto

Entradas:

- ✓ Inventário das lições aprendidas
- ✓ Tabela de fatores de riscos

Saídas:

- ✓ Tabela de escala de impacto

Descrição da atividade:

- ✓ Definir o nível de impacto no objetivo (do projeto, da contratação ou do processo de trabalho avaliado). Para tanto, devem ser consideradas as dimensões custo, prazo, escopo e qualidade. O impacto está associado às consequências do evento, conforme modelo apresentado na tabela a seguir:

IMPACTO NAS DIMENSÕES DO OBJETIVO				
CUSTO (aumento %)	**PRAZO (atraso %)**	**ESCOPO (afetação)**	**QUALIDADE (degradação)**	**NÍVEL**
Até 5	Até 5	Insignificante	Irrisória	1
> 5 Até 10	> 5 Até 10	Pouco	Pouco	2
> 10 Até 15	> 10 Até 15	Significativa	Relevante	3
> 15 Até 20	> 15 Até 20	Muito significativa	Muito relevante	4
> 20	>20	Ampla	Grave	5

O proprietário de Risco pode, quando necessário, adequar somente os quantitativos das colunas “custo” e “prazo”, a depender do caso concreto.

A escala de impacto pode variar de “muito baixo” a “muito alto”.

ESCALA DE IMPACTO		
DESCRITOR	**DESCRIÇÃO**	**NÍVEL**
Muito baixa	Impacto insignificante nos objetivos	1
Baixa	Impacto mínimo nos objetivos	2
Média	Impacto mediano nos objetivos, com possibilidade de recuperação	3

Alta	Impacto significante nos objetivos, com possibilidade remota de recuperação	4
Muito Alta	Impacto máximo nos objetivos, sem possibilidade de recuperação	5

Observações:

- ✓ Nem sempre o nível será o mesmo para todas as dimensões (custo, prazo, escopo e qualidade). Caso isso aconteça, deve ser considerado o maior nível de impacto dentre as dimensões.

Materiais auxiliares:

- ✓ Sem informação

Processo:
Estabelecimento do contexto geral

Atividade:

6. Estabelecer matriz de classificação de riscos

Entradas:

- ✓ Tabela de escala de probabilidade
- ✓ Tabela de escala de impacto

Saídas:

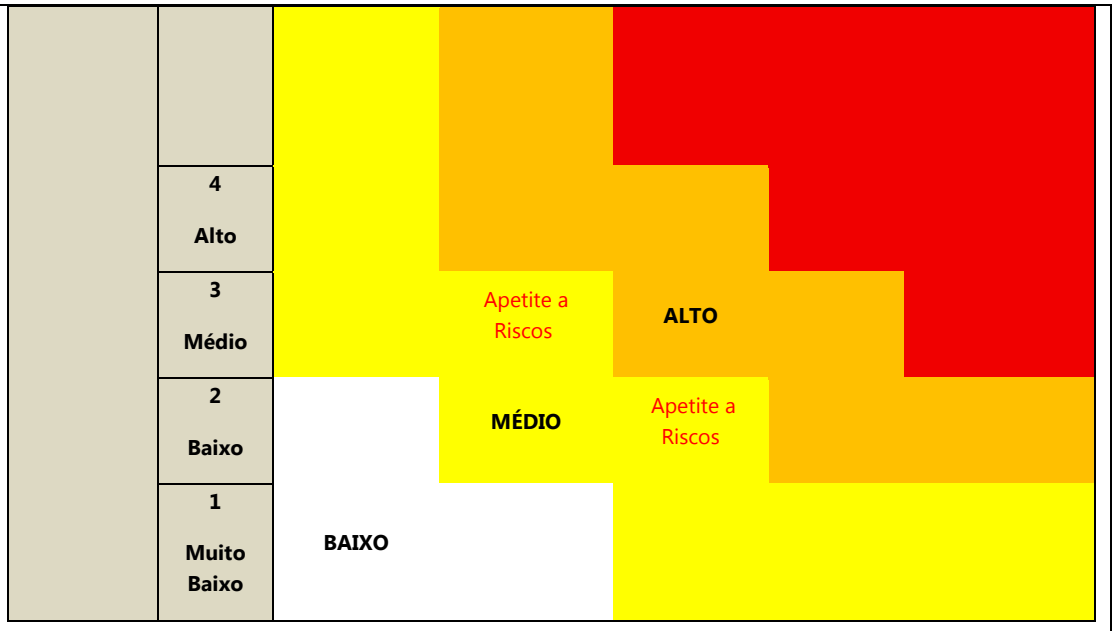
- ✓ Matriz de classificação de riscos

Descrição da atividade:

- ✓ Estabelecer a matriz de classificação de riscos que permita indicar o nível de risco por meio do cruzamento da escala de probabilidade com a escala de impacto.
- ✓ Destacar na matriz qual o nível máximo de risco que a unidade está disposta a assumir, ou seja, o seu Apetite a Riscos.

Exemplo de Matriz de classificação de riscos:

LEGENDA NÍVEL DE RISCO EXTREMO ALTO MÉDIO BAIXO		PROBABILIDADE				
		1 Muita Baixa	2 Baixa	3 Média	4 Alta	5 Muito Alta
IMPACTO	5 Muito Alto			EXTREMO		



Observações:

- ✓ Sem informação

Materiais auxiliares:

- ✓ Sem informação

Processo:
Estabelecimento do contexto geral

Atividade:

7. Pesquisar e formular um modelo do plano de gestão de riscos

Entradas:

- ✓ Planos de gestão de riscos de outros órgãos públicos
- ✓ Inventário de lições aprendidas

Saídas:

- ✓ Modelo do plano de gestão de riscos

Descrição da atividade:

- ✓ Propor um modelo (*template)* do plano de gestão de riscos, que possibilite a coleta de dados tais como:
  - Categorização do risco
  - Causa do risco
  - Evento
  - Consequência do risco
  - Medida de probabilidade
  - Medida de impacto
  - Nível do risco
  - Descrição dos controles internos
  - Eficácia dos controles internos
  - Risco residual
  - Resposta ao risco
  - Descrição de ações de prevenção
  - Relação custo/benefício das ações (favorável/desfavorável)

- Responsável pela implementação das ações de prevenção
- Prazo para implementação das ações de prevenção
- Descrição das ações de contingência
- Responsável pelas ações de contingência
- Condições (gatilhos) para adoção de ações de contingência

Observações:

- ✓ Sem informação

Materiais auxiliares:

- ✓ Sem informação

Processo:
Estabelecimento do contexto geral

Atividade:

8. Divulgar o contexto geral

Entradas:

- ✓ Artefatos produzidos neste processo:
  - Relação contendo os objetos designados para o plano de gestão de riscos
  - Matriz de classificação de riscos
  - Modelo do plano de gestão de riscos
- ✓ Política e demais artefatos atinentes à gestão de riscos de TIC.

Saídas:

- ✓ Artefatos produzidos neste processo publicados na Intranet
- ✓ Comunicado às unidades internas informando o contexto geral definido

Descrição da atividade:

- ✓ Publicar na intranet e se possível na Internet, todo o material necessário à formulação dos planos para gerenciamento de riscos pelos proprietários de riscos.

Observações:

- ✓ Sem informação

Materiais auxiliares:

- ✓ Sem informação

Processo: Gerenciamento de riscos
Atividade: 1. Avaliar lições aprendidas
Entradas: ✓ Informações coletadas em repositório de lições aprendidas (Por exemplo o SEI, Sistema de Ger. de Projetos) e/ou em entrevistas e reuniões com os gerentes de projetos e processos.
Saídas: ✓ Inventário de lições aprendidas extraídas do portfólio de projetos e dos processos de TIC
Descrição da atividade: ✓ Avaliar lições aprendidas de contextos similares, quando houver.
Observações: ✓ Sem informação
Materiais auxiliares: ✓ Sem informação

Processo: Gerenciamento de riscos
Atividade: 2. Estabelecer o contexto específico
Entradas: ✓ Inventário de lições aprendidas extraídas do portfólio de projetos e dos processos de TIC ✓ Tabela com a categorização de fatores de riscos internos e externos à TIC produzida no processo de estabelecimento do contexto geral.
Saídas: ✓ Tabela dos fatores externos e internos aplicável ao contexto específico ✓ Tabela de escala de probabilidade aplicável ao contexto específico ✓ Tabela de escala de impacto aplicável ao contexto específico
Descrição da atividade: ✓ Identificar com base no contexto geral estabelecido, os fatores externos e internos que devem ser levados em consideração para gerenciar os riscos no contexto específico (caso concreto). ✓ Adaptar, caso necessário, os critérios de riscos definidos no contexto geral (tabela de escala de probabilidade e tabela de escala de impacto)
Observações: ✓ O proprietário do risco deverá ajustar as categorias de eventos estabelecidos no contexto geral, excluindo as que não se aplicam ao caso concreto e incluindo as que não estiverem previstas.

Materiais auxiliares:

- ✓ Sem informação

Processo:
Gerenciamento de riscos

Atividade:

3. Identificar os riscos

Entradas:

- ✓ Tabela dos fatores externos e internos aplicável ao contexto específico
- ✓ Inventário de lições aprendidas extraídas do portfólio de projetos e dos processos de TIC

Saídas:

- ✓ Plano de gestão de riscos de TIC atualizado com os riscos identificados

Descrição da atividade:

- ✓ Identificar os riscos que possam influenciar os objetivos estabelecidos. Para o desempenho dessa atividade pode-se utilizar técnicas como *brainstorming*, questionários, entrevistas, análise de dados históricos, dentre outros.
  - Uma abordagem promissora para essa atividade é a análise *top-down*, a partir dos processos/projetos mais críticos para o TRE-RO. Após a definição do objeto da análise, faz-se o inventário dos ativos que o sustentam e a análise de suas vulnerabilidades. Na análise das vulnerabilidades dos ativos serão identificados os riscos, que em graus variados ameaçam os ativos e consequentemente os objetivos da instituição.

Observações:

- ✓ Exemplo de identificação de riscos:

PROCESSO DE TRABALHO	Planejamento de Contratação de Solução de TIC			
OBJETIVO DO PROCESSO DE TRABALHO	Elaborar o Termo de Referência necessário à contratação, em conformidade com a legislação vigente			
ID	**CAUSA**	**EVENTO**	**CONSEQUÊNCIA**	**CATEGORIA**
1	Não observância de requisitos definidos na Lei nº 10.520/2002;	Provimento do pedido de impugnação do edital	Atraso na realização da contratação pretendida	CONFORMIDADE
N				

Materiais auxiliares:

- ✓ Sem informação

Processo:
Gerenciamento de riscos

Atividade:
4. Analisar os riscos

Entradas:
- ✓ Plano de gestão de riscos de TIC, preenchido com os riscos identificados

Saídas:
- ✓ Plano de gestão de riscos de TIC, atualizado com informações de probabilidade e impacto de ocorrência dos eventos.

Descrição da atividade:
- ✓ Definir os níveis de probabilidade e de impacto de cada risco identificado, mediante a compreensão de sua natureza, do histórico de ocorrências e do impacto nas dimensões custo, prazo e qualidade do objetivo pretendido. Deverão ser consideradas as escalas de probabilidade e de impacto previamente definidas.

Observações:
- ✓ Para definir o nível de impacto, recomenda-se, primeiramente, avaliar quais dimensões, dentre custo, prazo, escopo e qualidade, do objetivo serão influenciadas em uma provável ocorrência do evento de risco.

Materiais auxiliares:
- ✓ Sem informação

Processo:
Gerenciamento de riscos

Atividade:
5. Avaliar os riscos

Entradas:
- ✓ Plano de gestão de riscos de TIC, atualizado com informações de probabilidade e impacto de ocorrência dos eventos.

Saídas:
- ✓ Plano de gestão de riscos de TIC, atualizado com recomendações para tratamento.

Descrição da atividade:
- ✓ Relacionar os resultados aferidos na atividade anterior, multiplicando o valor obtido para a probabilidade de ocorrência do evento, pelo valor obtido para o impacto desse evento. O resultado dessa multiplicação é o chamado nível do risco.
- ✓ Verificar a existência de controles existentes e atribuir o valor chamado de risco de controle, conforme a tabela de eficácia dos controles mais adiante.
- ✓ Multiplicar o nível do risco pelo risco de controle, a fim de obter o risco residual.

Tabela de Eficácia dos Controles

Situação observada do controle	Nível de Avaliação do controle	Nível de confiança nos controles	Risco de controle

Inexistente ou não funcional/não implementado	Inexistente	0%	1,00
Não formalizado, baseado no conhecimento dos operadores, em geral realizado manualmente	Fraco	20%	0,80
Razoavelmente formalizado, seu desenho ou ferramentas não são adequados para suporte de todos os riscos relevantes	Mediano	40%	0,60
Formalizado mas pode ser aperfeiçoado, ferramentas adequadas e mitiga os riscos razoavelmente	Satisfatório	60%	0,40
Formalizado e sustentado por ferramentas adequadas, mitiga os riscos em todos os aspectos relevantes e pode ser considerado como paradigma de melhores práticas.	Forte	80%	0,20

Exemplo do Plano de Riscos preenchido com as informações obtidas até este ponto do processo:

Processo de Trabalho	Planejamento de Contratação de Solução de TIC
Objetivo do Processo de Trabalho	Elaborar o Termo de Referência necessário à contratação, em conformidade com a legislação vigente

RISCOS IDENTIFICADOS				**AVALIAÇÃO DO RISCO INERENTE**			**CONTROLES EXISTENTES**			**RISCO RESIDUAL**	**RECOMENDAÇÃO PARA TRATAMENTO DO RISCO**	
ID	**Eventos**	**Causas**	**Consequências**	**Proba-bilidade**	**Impacto**	**Nível**	**Descrição**	**Eficácia**			**Diretriz**	Resposta ao risco
1	Provimento do pedido de impugnação do edital	Não observância de requisitos definidos na Lei nº 10.520/2002;	Atraso na realização da contratação pretendida	4	5	**20**	Revisão do documento baseada na experiência	Fraco	**0,8**	**12,0**	Alto	Mitigar

Observações:

- ✓ É com base no risco residual que serão planejadas as ações preventivas ou de mitigação.

Materiais auxiliares:

- ✓ Sem informação

Processo:
Gerenciamento de riscos
Atividade:

6. Planejar ações de tratamento dos riscos

Entradas:

- ✓ Plano de gestão de riscos de TIC, atualizado com recomendações para tratamento.
- ✓ Se houver: Ata de reunião do CETIC com decisão de resposta aos riscos
- ✓ Se houver: Ata de reunião do CDTIC com decisão de resposta aos riscos

Saídas:

- ✓ Plano de gestão de riscos de TIC, atualizado com os tipos de respostas e com as ações de tratamento.

Descrição da atividade:

- ✓ Registrar no plano de gestão de riscos de TIC os tipos de resposta, as ações de tratamento aos riscos e, ainda, os responsáveis e os prazos de execução correspondentes, quer sejam riscos da alçada do próprio Proprietário de Riscos ou não. Neste caso, registrar as ações de tratamento deliberadas nos respectivos Comitês (CETIC ou CDTIC).

Observações:

- ✓ Uma vez consolidado o plano de gestão de riscos de TIC, o mesmo deverá ser encaminhado à unidade de apoio à governança de TIC ou equivalente, para fins de integração, monitoramento e reporte ao CETIC.

Materiais auxiliares:

- ✓ Sem informação.

Processo:
Gerenciamento de riscos

Atividade:

7. Deliberar sobre riscos na alçada do CETIC

Entradas:

- ✓ Plano de gestão de riscos de TIC, atualizado com recomendações para tratamento.

Saídas:

- ✓ Ata de reunião do CETIC com decisão de resposta aos riscos

Descrição da atividade:

- ✓ Analisar todos os riscos reportados pelo Proprietário, principalmente os considerados médios e altos cujo estabelecimento das ações de tratamento estiver acima da competência e autoridade do Proprietário de Riscos.
- ✓ Analisar as opções de tratamento, ponderando a relação custo/benefício.
- ✓ Estabelecer respostas aos riscos, conforme descrito a seguir:

Evitar - objetiva descontinuar as atividades que geram o risco. “No setor público é quase impossível optar por essa opção, dado que é da sua natureza assumir riscos que os próprios cidadãos não podem assumir individualmente” (TCU);
Transferir - objetiva compartilhar ou transferir uma parte do risco a terceiros, assim como a responsabilidade pela sua resposta. Nem todos os riscos são totalmente transferíveis, a exemplo dos riscos associados à reputação ou à imagem;
Mitigar - objetiva reduzir a probabilidade de um evento de risco adverso, o seu impacto ou ambos, para dentro de limites aceitáveis;
Aceitar - objetiva reconhecer a existência do risco e não agir, a menos que o risco ocorra, torne-se um problema. Antes disso, deve ser avaliado se os demais tipos de

resposta ao risco são viáveis. Em algumas situações, como risco de nível baixo ou custo desproporcional ao benefício do tratamento, a opção mais adequada é aceitar ou reter o risco.

- ✓ Para os casos em que se optou pela aceitação do risco, é recomendável que o proprietário do risco elabore pelo menos um plano de contingência viável para atenuar os impactos.
- ✓ Comunicar decisão ao Proprietário do risco, caso este não tenha participado da deliberação junto com o CETIC.

Observações:

- ✓ Em caso de riscos extremos e/ou residuais altos, o CETIC deverá reportá-los ao CDTIC, após avaliação técnica, incluindo propostas de ações a serem adotadas.
- ✓ O encaminhamento anterior, ou seja, escalonamento ao CDTIC, também se aplica quando as opções de tratamento resultarem em uma relação custo/benefício desfavorável. Nesses casos, o encaminhamento precisa ocorrer com a manifestação do CETIC propondo como resposta mais adequada a ação de evitar (se possível) ou aceitar o risco.

Materiais auxiliares:

- ✓ Sem informação

Processo:
Gerenciamento de riscos

Atividade:

8. Deliberar sobre riscos na alçada do CDTIC

Entradas:

- ✓ Plano de gestão de riscos de TIC, atualizado com as recomendações para tratamento.
- ✓ Ata de reunião do CETIC com proposta ações de resposta aos riscos

Saídas:

- ✓ Ata de reunião do CDTIC com decisão de resposta aos riscos

Descrição da atividade:

- ✓ Analisar todos os riscos reportados pelo Proprietário e pelo CETIC.
- ✓ Analisar as opções de tratamento, ponderando a relação custo/benefício.
- ✓ Estabelecer respostas aos riscos (Evitar, Transferir, Mitigar ou Aceitar) conforme descrito na atividade anterior.
- ✓ Comunicar decisão ao CETIC e ao Proprietário do risco, caso este não tenha participado da deliberação.

Observações:

- ✓ Sem informação

Materiais auxiliares:

- ✓ Sem informação

Processo:
Gerenciamento de riscos

Atividade:

9. Implementar as ações de tratamento

Entradas: ✓ Plano de gestão de riscos de TIC
Saídas: ✓ Relatório de ações implementadas ✓ Registro dos riscos residuais atualizados
Descrição da atividade: ✓ Implementar as ações mitigatórias dos riscos ✓ Atualizar registros, informando os riscos residuais após a implementação das ações o Caso os riscos residuais estejam acima da tolerância ao risco planejar novas ações de tratamento. ✓ Informar à unidade apoio à Governança de TIC ou equivalente, para fins de integração, monitoramento e reporte ao CETIC.
Observações: ✓ O tratamento de riscos, por si só, pode introduzir riscos. Um risco significativo pode derivar do fracasso ou ineficácia das medidas de tratamento de riscos. O monitoramento precisa fazer parte do plano de tratamento de forma a garantir que as medidas permaneçam eficazes.[1]
Materiais auxiliares: ✓ Sem informação

Processo: Gerenciamento de riscos
Atividade: 10. Monitorar os riscos do objeto
Entradas: ✓ Plano de gestão de riscos de TIC
Saídas: ✓ Informação periódica sobre o monitoramento
Descrição da atividade: ✓ Monitorar o projeto ou contratação até sua conclusão. Caso se trate de um processo o seu monitoramento deve ser mantido até a sua descontinuidade. Em ambas as situações, caso seja identificado um novo risco ou alterações no nível do risco (aumento de probabilidade/impacto), este processo de gerenciamento de riscos precisa ser reexecutado para atualização do plano de gestão de riscos. ✓ Emitir periodicamente informação sobre a continuidade do processo ou projeto e sobre os novos riscos identificados, alteração nos níveis de riscos ou condições (gatilhos) que ensejam a adoção de ações de contingência.
Observações: ✓ Sem informação
Materiais auxiliares: ✓ Sem informação

[1] ABNT, Associação Brasileira de Normas Técnicas, **ABNT NBR ISO 31000**: Gestão de Riscos – Princípios e Diretrizes, Rio de Janeiro, 2009.

Processo: Integração e Análise Crítica
Atividade: 1. Integrar o monitoramento dos riscos
Entradas: ✓ Plano de gestão de riscos de TIC ✓ Informações dos proprietários de riscos sobre o monitoramento dos projetos/processos
Saídas: ✓ Informação periódica sobre o monitoramento integrado
Descrição da atividade: ✓ Solicitar as informações dos proprietários ✓ Integrar as informações em repositório apropriado ✓ Emitir informação periódica ao CETIC sobre o monitoramento integrado, contendo pelo menos a relação de processos e projetos monitorados com os respectivos proprietários de riscos e eventuais apontamentos feitos por estes.
Observações: ✓ Sem informação
Materiais auxiliares: ✓ Sem informação

Processo: Integração e Análise Crítica
Atividade: 2. Analisar criticamente
Entradas: ✓ Plano de gestão de riscos de TIC ✓ Informação periódica sobre o monitoramento integrado
Saídas: ✓ Ata de reunião do CETIC sobre a análise do monitoramento dos riscos de TIC
Descrição da atividade: ✓ Analisar criticamente o plano de gestão de riscos de TIC, levantando a ocorrência de novos riscos passíveis de inclusão no plano, bem como alterações no ambiente que ensejam mudanças no nível de riscos. Considerar as seguintes fontes: o Informação periódica sobre o monitoramento integrado; o Lições aprendidas; o Relatórios de auditoria; o Atas de Reuniões de Análise da Estratégia.
Observações: ✓ Sem informação
Materiais auxiliares: ✓ Sem informação

Processo: Integração e Análise Crítica
Atividade: 3. Comunicar
Entradas: ✓ Ata de reunião do CETIC sobre a análise do monitoramento dos riscos de TIC
Saídas: ✓ Relatório para o CDTIC
Descrição da atividade: ✓ Consolidar as informações da ata de reunião do CETIC sobre a análise do monitoramento dos riscos de TIC. ✓ Elaborar relatório com informações relevantes que possam implicar atualização no processo de gestão de riscos e/ou na política de gestão de riscos; na necessidade de recursos adicionais, de capacitação, etc.
Observações: ✓ Sem informação
Materiais auxiliares: ✓ Sem informação

5. Papéis e Responsabilidades

O Secretário de Tecnologia da Informação irá desempenhar o papel de dono do presente processo. O dono do processo é o papel com a responsabilidade de garantir que o processo é adequado ao propósito, devendo atuar no seu patrocínio, desenho, gerenciamento de mudanças e na promoção da sua melhoria continuada.

Além do dono, os demais papéis e responsabilidades envolvidos com o processo de Gestão de Riscos de TIC, foram reunidos na matriz RACI a seguir:

PROCESSO: ESTABELECIMENTO DO CONTEXTO					
Atividade	CDTIC	CETIC	SEGOVTIC	Gerentes de projetos	Gerentes de processos
Identificar os objetos relevantes		R			
Avaliar lições aprendidas		R		C	C

Estabelecer os fatores internos e externos		R			
Estabelecer a escala de probabilidade		R			
Estabelecer a escala de impacto		R			
Estabelecer matriz de classificação de riscos	A	R		I	I
Pesquisar e formular um modelo do plano de gestão de riscos		A	R	I	I
Divulgar o contexto geral		A	R	I	I

PROCESSO: GERENCIAMENTO DE RISCOS			
Atividade	CDTIC	CETIC	Proprietário de Risco
Avaliar lições aprendidas			R
Estabelecer o contexto específico		I	R
Identificar os riscos		I	R
Analisar os riscos		I	R
Avaliar os riscos		I	R
Deliberar sobre riscos na alçada do CETIC		R	C
Deliberar sobre riscos na alçada do CDTIC	R	C	C
Planejar ações de tratamento dos riscos			R
Implementar as ações de tratamento		I	R
Monitorar os riscos do objeto		I	R

PROCESSO: INTEGRAÇÃO E ANÁLISE CRÍTICA			
Atividade	CETIC	SEGOVTIC	Proprietário de Risco
Integrar o monitoramento dos riscos	I	R	C
Analisar criticamente	R	I	I
Comunicar		R	I

6. Metas e métricas

Foram definidas as seguintes métricas para avaliar o processo:

Identificador	RISCOSTIC-01
Dono do Processo	Secretário de Tecnologia da Informação e Comunicação
Indicador ou Índice	Integração dos processos à Gestão de Riscos de TIC
Justificativa	Medir a efetiva aplicação do processo nos objetos designados para gestão dos riscos
Periodicidade de medição	Anual
Regra de apuração	$\frac{Qtd.\ de\ objetos\ que\ passaram\ a\ integrar\ o\ plano\ de\ gestão\ de\ riscos\ de\ TIC\ no\ ano \times 100}{Qtd.\ de\ objetos\ designados\ para\ integrar\ o\ plano\ de\ gestão\ de\ riscos\ de\ TIC}$ Onde: → Os objetos da gestão de riscos podem ser: processos de trabalho; projetos; iniciativas ou planos de ação. → A quantidade de processos designados para ser integrado à gestão de riscos dever ser estabelecida no início do ano pelo CETIC
Meta	100%
Polaridade da meta	Melhor se maior
Origem dos dados (sistema de coleta)	✓ Plano de Gestão de Riscos de TIC ✓ Sistema de Gerenciamento de Projetos ✓ Planilhas de controle
Responsável pela coleta	SEGOVTIC
Responsável pela validação do indicador apurado	CETIC

Identificador	RISCOSTIC-02
Dono do Processo	Secretário de Tecnologia da Informação e Comunicação
Indicador ou Índice	Indicador de relacionamento entre incidentes graves e controles internos identificados na gestão de riscos de TIC
Justificativa	Medir a efetividade do plano de gestão de riscos na prevenção de incidentes graves.
Periodicidade de medição	Anual
Regra de apuração	Qtd. de incidentes graves decorrentes de falhas em controles internos apontados no plano de gestão de riscos.

Meta	0 (zero)
Polaridade da meta	Manter o nível estabelecido na meta
Origem dos dados (sistema de coleta)	✓ Processo SEI de registro de incidentes graves ✓ OTRS ✓ Plano de Gestão de Riscos de TIC
Responsável pela coleta	SEGOVTIC
Responsável pela validação do indicador apurado	CETIC

7. Relacionamento com outros processos

O atual processo deve ser integrado em todos os processos de TIC, principalmente aqueles que afetam a **segurança da informação e os serviços críticos de TIC da Instituição.**

8. Modelos de Referência

Constituem modelos de referência para o processo de Gestão de Riscos de TIC, os seguintes:

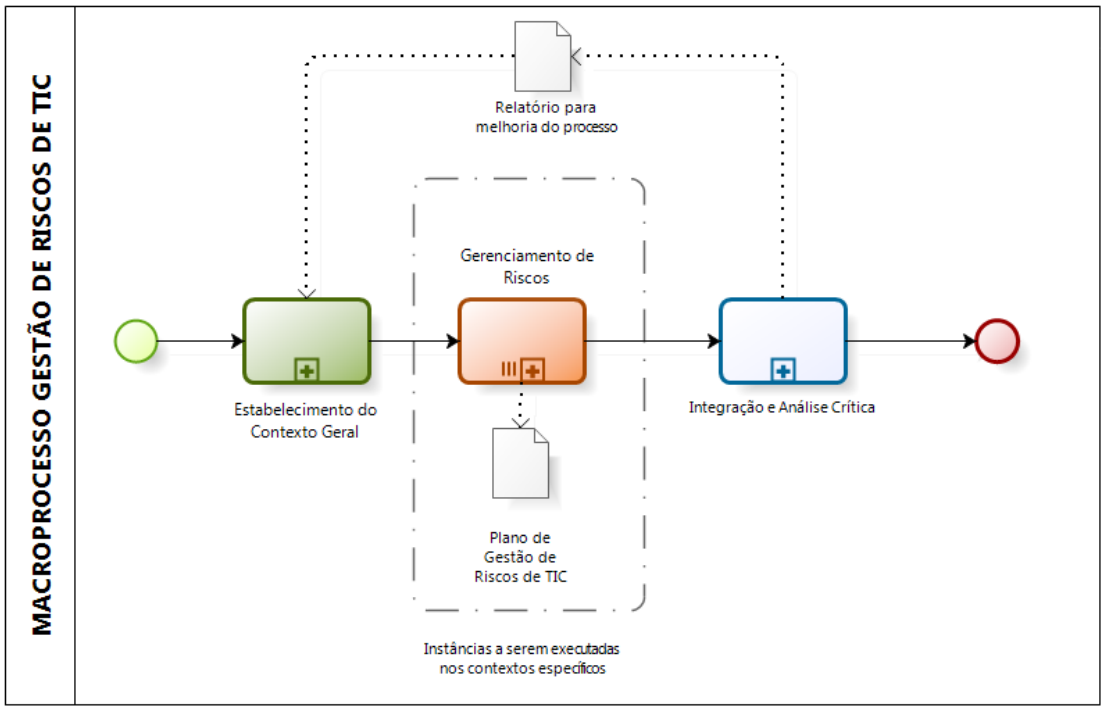
- Resolução TRE-RO nº 05/2017 (Política de Gerenciamento de Riscos)
- Resolução TRE-RO nº 20/2019 (Política de Gestão de Riscos de TIC)
- Norma ABNT ISO 73:2009
- Norma ABNT NBR ISO/IEC 27.005:2011
- Norma ABNT NBR ISO 31.000:2018
- COSO-ERM

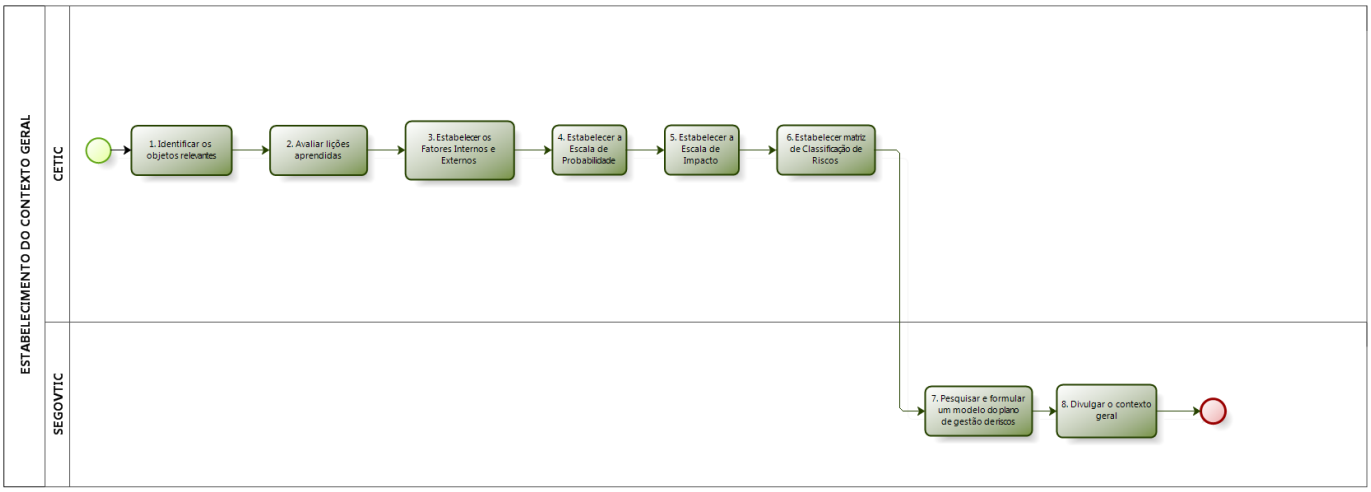
9. Revisão

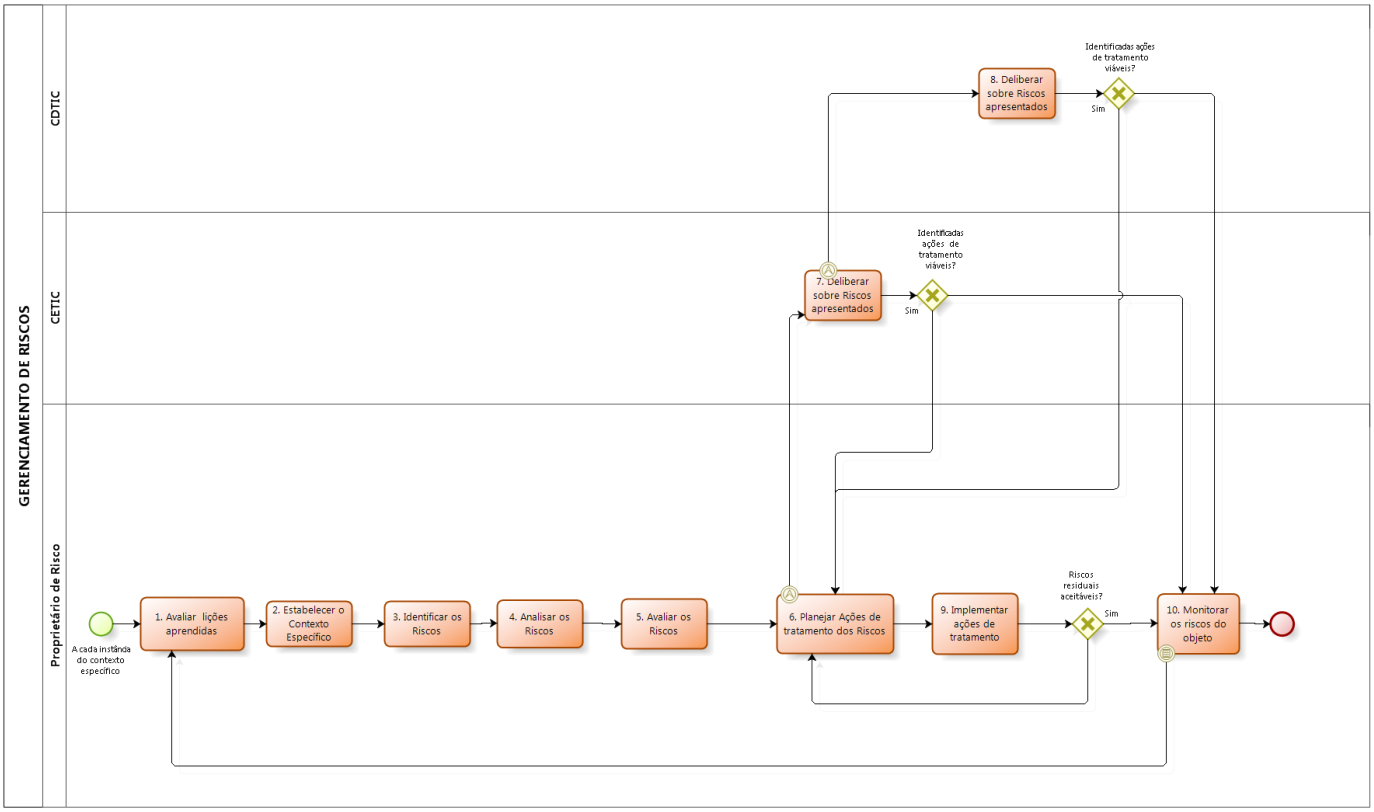
Este manual de processo deverá ser revisto ordinariamente em intervalos de até 4 anos ou extraordinariamente por determinação dos comitês de governança (CDTIC ou CETIC).

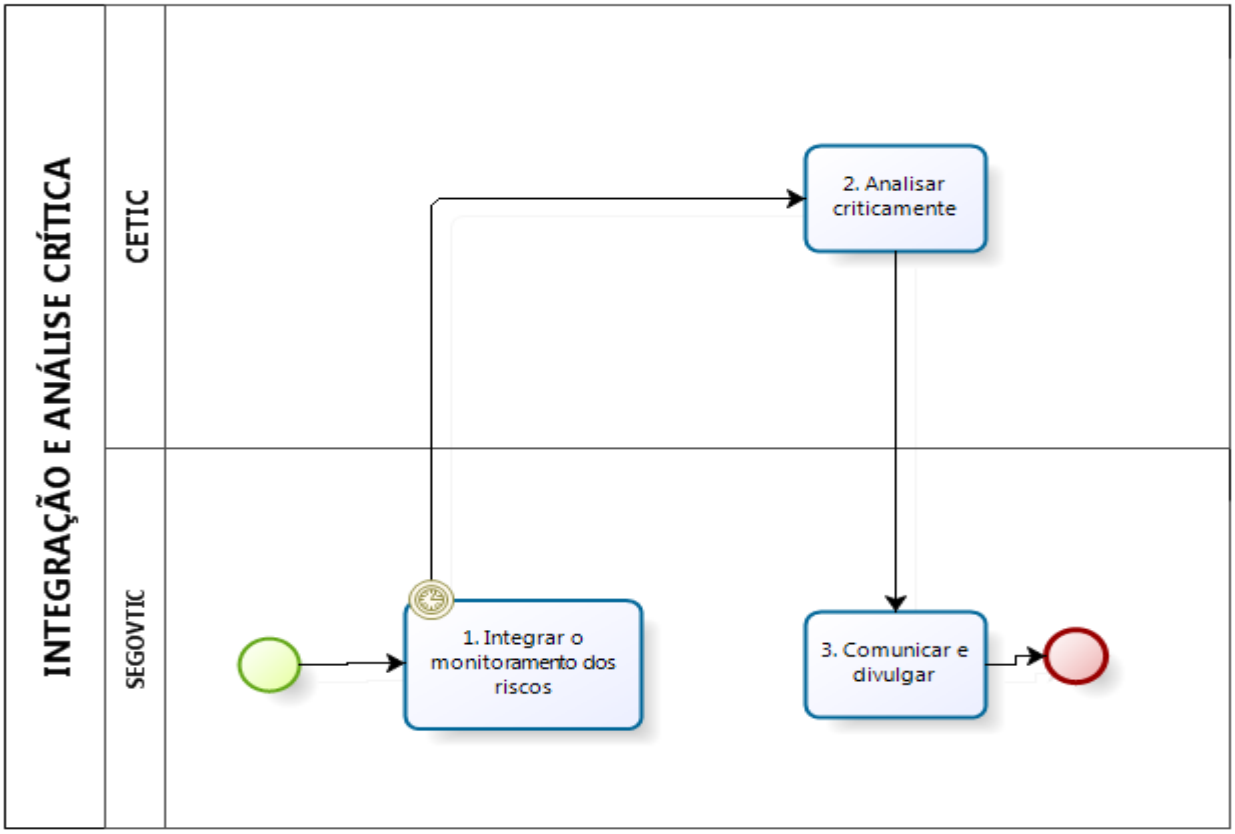
10. Diagramas do processo

Os diagramas do processo, foram elaborados no nível descritivo de abstração e estão dispostos a seguir.






GERENCIAMENTO DE RISCOS
CDTIC
CETIC
Proprietário de Risco
A cada instância do contexto específico
1. Avaliar lições aprendidas
2. Estabelecer o Contexto Específico
3. Identificar os Riscos
4. Analisar os Riscos
5. Avaliar os Riscos
6. Planejar Ações de tratamento dos Riscos
7. Deliberar sobre Riscos apresentados
Identificadas ações de tratamento viáveis?
Sim
8. Deliberar sobre Riscos apresentados
Identificadas ações de tratamento viáveis?
Sim
9. Implementar ações de tratamento
Riscos residuais aceitáveis?
Sim
10. Monitorar os riscos do objeto


INTEGRAÇÃO E ANÁLISE CRÍTICA
CETIC
SEGOVTIC
2. Analisar criticamente
1. Integrar o monitoramento dos riscos
3. Comunicar e divulgar