MANUAL DE PROCESSO DE TRABALHO 34

IDENTIFICAÇÃO DO PROCESSO

PROCESSO DE GESTÃO DE RISCOS DE TI		
OBJETIVO	Identificar, analisar, avaliar, tratar, monitorar e comunicar potenciais eventos ou situações que possam afetar o alcance dos objetivos de ação, processo ou projeto avaliado.	
MANUAL	**NÚMERO**	34
	NOME	RISCOS DE TI
	VERSÃO	1

VISÃO SISTÊMICA

PROCESSO DE GESTÃO DE RISCOS DE TI	
ENTRADA(S)	Relação das partes interessadas Objetivos de negócio e de TI Legislação relacionada Avaliações de riscos anteriores
FORNECEDOR(ES)	Partes interessadas Planejamento Estratégico de TI Planejamento Estratégico Institucional
SAÍDA(S)	Riscos de TI identificados e tratados Partes interessadas cientes dos riscos de TI
CLIENTE(S)	Eleitores Unidades da Secretaria Corregedoria Cartórios Eleitorais
REGULAÇÃO	Resolução TRE-SE 17/2018
RECURSO(S)	Sistema Eletrônico de informações

CADEIA DE VALOR

POSIÇÃO DO PROCESSO NA CADEIA DE VALOR	
MACROPROCESSO DE APOIO	Os macroprocessos de apoio garantem o suporte adequado aos processos finalísticos
MACROPROCESSO 10	Gestão de Tecnologia da Informação e Comunicação
PROCESSO 10.1	Administração da Infraestrutura de TIC
SUBPROCESSO 10.1.20	Gestão de Riscos de TI

GESTOR DO PROCESSO

GESTOR DO PROCESSO	
UNIDADE	A Assessoria de Planejamento e Gestão da STI (ASPLAN/STI) é a unidade responsável pela gestão do processo, cabendo-lhe seu acompanhamento, controle e melhoria. Esta unidade também receberá as dúvidas e sugestões acerca do processo para análise e providências necessárias.

PARTICIPANTE(S) DO PROCESSO

PARTICIPANTE(S)	
EQUIPE DE GESTÃO DE RISCOS (EGR)	Equipe multidisciplinar, formada por servidores da STI, responsável por identificar, analisar, avaliar, tratar, monitorar e comunicar potenciais eventos ou situações que possam afetar o alcance dos objetivos da ação, processo ou projeto avaliado.
COMITÊ DE GESTÃO DE TI (CGESTI)	Órgão colegiado, formado por membros da área de TI, responsável pela tomada de decisão acerca das atividades de planejamento, coordenação, supervisão e controle das soluções de tecnologia da informação (TI).
COMITÊ DE GOVERNANÇA DE TI (CGOVTI)	Órgão colegiado, formado por membros das áreas finalísticas e da área de TI, que tem o objetivo de promover a entrega de valor por meio da TI e do uso estratégico da informação na organização. Cuida para que a formulação e a implementação das estratégias e planos de TI estejam harmonizadas com os objetivos organizacionais de alto nível.
GESTORES DE RISCOS	Os responsáveis pelas unidades administrativas, pelos processos de trabalho, projetos e ações desenvolvidas nos níveis estratégicos, táticos ou operacionais da Secretaria de Tecnologia da Informação (STI).

TERMOS E DEFINIÇÕES

TERMO	DEFINIÇÃO
ANÁLISE DE RISCOS	Processo de compreender a natureza e determinar o nível (magnitude, severidade) de um risco ou combinação de riscos, mediante a combinação das consequências e de suas probabilidades.
AVALIAÇÃO DE RISCOS	Processo de comparar os resultados da análise de riscos com os critérios de risco da organização, para determinar se um risco e/ou sua magnitude é aceitável ou tolerável.
CONSEQUÊNCIA	Resultado de um evento que afeta positiva ou negativamente os objetivos da organização.
EVENTO	Um incidente ou uma ocorrência de fontes internas ou externas à organização, que podem impactar a implementação da estratégia e a realização de objetivos de modo negativo, positivo ou ambos.
FONTE DE RISCO	Elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco.
GERENCIAMENTO DE RISCOS	Aplicação de uma arquitetura (princípios, estrutura e processo) para identificar riscos, analisar e avaliar se devem ser modificados por algum tratamento a fim de atender critérios de risco. Ao longo desse processo, comunica-se e consulta-se as partes interessadas, monitora-se e analisa-se criticamente os riscos e os controles que os modificam, a fim de assegurar que nenhum tratamento de risco adicional é requerido.
IDENTIFICAÇÃO DE RISCOS	Processo de busca, reconhecimento e descrição de riscos. Envolve a identificação das fontes de risco, os eventos, suas causas e suas consequências potenciais. Pode envolver, ainda, a análise de dados históricos, análises teóricas, opiniões de pessoas informadas e de especialistas e as necessidades das partes interessadas.

TERMO	DEFINIÇÃO
MAPA DE PROCESSO	Representação gráfica da sequência de atividades que compõem um processo, fornecendo uma visão dos fluxos operacionais do trabalho, incluindo, a depender do nível de análise que se deseja realizar, a evidenciação dos agentes envolvidos, os prazos, o fluxo de documentos e o processo decisório
MEDIDAS DE CONTINGÊNCIA	Ações previamente planejadas que devem ser executadas caso um ou mais riscos se concretizem.
MONITORAMENTO	Verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado. O monitoramento pode ser aplicado a riscos, a controles, à estrutura de gestão de riscos e ao processo de gestão de riscos.
NÍVEL DE RISCO	Magnitude de um risco ou de uma combinação de riscos, expressa em termos da combinação das consequências (impacto) e de suas probabilidades.
POLÍTICA DE GESTÃO DE RISCOS	Documento que contém a declaração das intenções e diretrizes gerais relacionadas à gestão de riscos e estabelece, claramente, os objetivos e o comprometimento da organização em relação à gestão de riscos. Não se trata de uma declaração de propósitos genérica, mas de um documento que, além de declarar os princípios, explica o motivo pelo qual a gestão de riscos é adotada; o que se pretende com ela; onde, como e quando ela é aplicada; quem são os responsáveis em todos os níveis, dentre outros aspectos.

TERMO	DEFINIÇÃO
RESPOSTAS A RISCO	Opções e ações gerenciais para tratamento de riscos. Inclui: - evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem mesmo, porque o risco está além do apetite a risco da organização e outra resposta não é aplicável; - transferir o risco a outra parte ou compartilhar o risco com outra parte; - aceitar o risco por uma escolha consciente; ou - mitigar o risco diminuindo sua probabilidade de ocorrência ou minimizando suas consequências.
RISCO	Possibilidade de um evento ocorrer e afetar adversamente a realização de objetivos; possibilidade de algo acontecer e ter impacto nos objetivos, sendo medido em termos de consequências e probabilidades; efeito da incerteza nos objetivos.
RISCO DE CONTROLE	Possibilidade de que os controles adotados pela administração não sejam eficazes para tratar o risco a que se propõe.
RISCO INERENTE	O risco intrínseco à natureza do negócio, do processo ou da atividade, independentemente dos controles adotados.
RISCO RESIDUAL	O risco retido de forma consciente ou não pela administração, que remanesce mesmo após o tratamento de riscos.
TRATAMENTO DE RISCOS	Processo de implementar respostas a risco selecionadas.

DOCUMENTO(S) DO PROCESSO

DOCUMENTO	NOME	ONDE É ENCONTRADO OU UNIDADE RESPONSÁVEL
D1	Contexto da Gestão de Riscos	ASPLAN-STI
D2	Planilha Matriz de Probabilidade x Impacto (MPI)	ASPLAN-STI
D3	Plano de Tratamento de Riscos (PTR)	ASPLAN-STI
D4	Relatório de Gestão de Riscos (RGR)	ASPLAN-STI

INDICADOR(ES) DE DESEMPENHO

INDICADOR: ÍNDICE DE PROCESSOS CRÍTICOS AVALIADOS	
TIPO	Eficácia
O QUE MEDE	O percentual de processos críticos de TI avaliados durante o ano.
PARA QUE MEDIR	Permite monitorar se os riscos dos processos críticos de TI estão sendo adequadamente identificados, gerenciados e tratados.
QUEM MEDE	ASPLAN/STI
QUANDO MEDIR	Anualmente
ONDE MEDIR	SEI

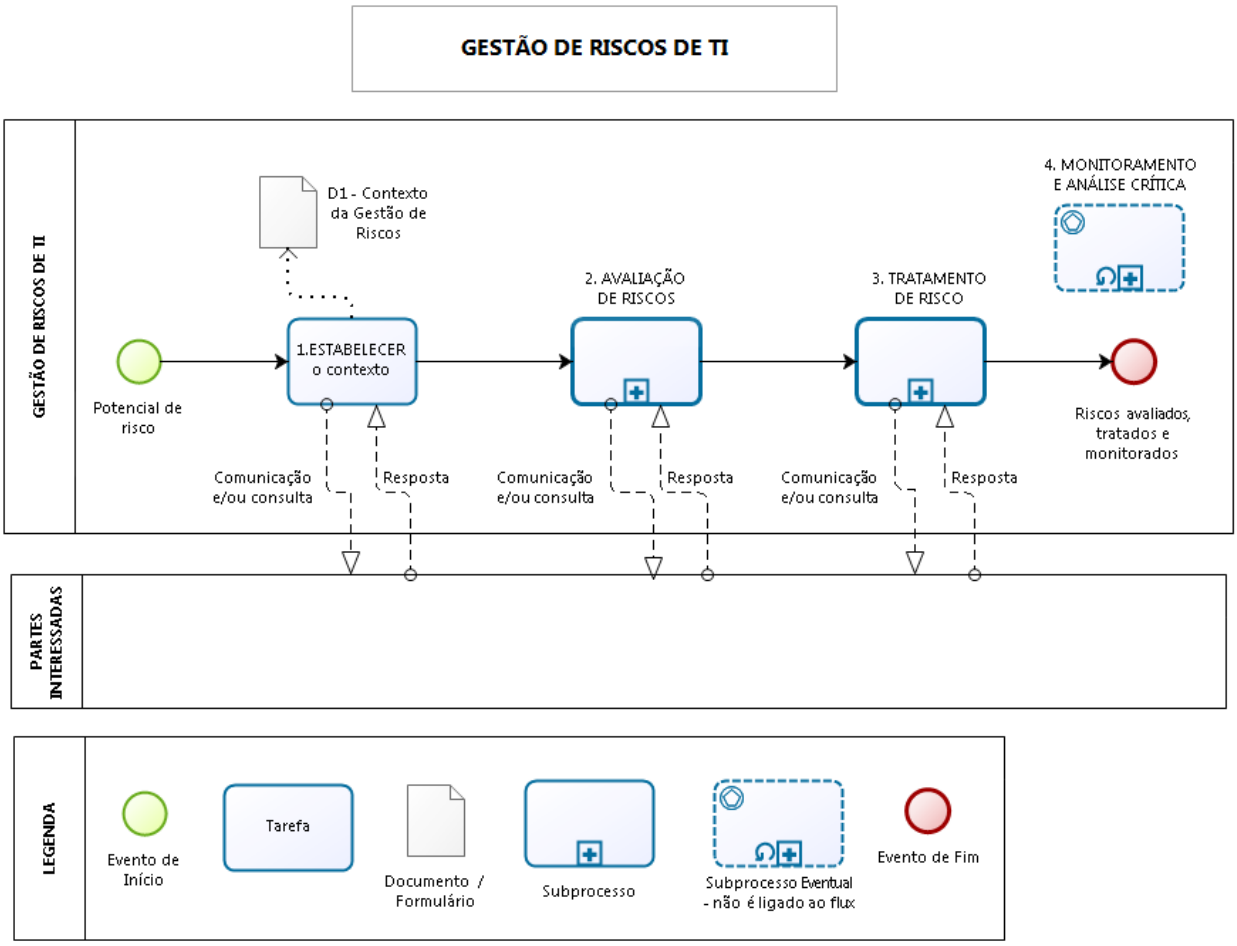
INDICADOR: ÍNDICE DE PROCESSOS CRÍTICOS AVALIADOS	
COMO MEDIR	Total de processos críticos avaliados no período (TPCA) dividido pelo total de processos do período (TPP), multiplicado por cem: (TPCA / TPP) x 100, onde: 1. O total de processos críticos avaliados (TPCA) representa o total de processos críticos de TI efetivamente avaliados no ano; 2. O total de processos do período (TPP) representa o total de processos críticos de TI escolhidos para serem analisados durante o ano.
META	50% dos processos críticos avaliados e tratados.

AUTORES DO MANUAL

MANUAL ELABORADO POR	
UNIDADES	STI - Secretaria de Tecnologia da Informação
	SEORG - Seção de Otimização de Processos Organizacionais

SOBRE A VERSÃO

VERSÃO	RESUMO DAS ALTERAÇÕES	RESPONSÁVEL
1	Versão inicial.	Autores do Manual


GESTÃO DE RISCOS DE TI
GESTÃO DE RISCOS DE TI
D1 - Contexto da Gestão de Riscos
4. MONITORAMENTO E ANÁLISE CRÍTICA
2. AVALIAÇÃO DE RISCOS
3. TRATAMENTO DE RISCO
1.ESTABELECER o contexto
Potencial de risco
Riscos avaliados, tratados e monitorados
Comunicação e/ou consulta
Resposta
Comunicação e/ou consulta
Resposta
Comunicação e/ou consulta
Resposta
PARTES INTERESSADAS
LEGENDA
Evento de Início
Tarefa
Documento / Formulário
Subprocesso
Subprocesso Eventual - não é ligado ao flux
Evento de Fim

ENTIDADES/PROCESSOS RELACIONADOS

PARTES INTERESSADAS
DESCRIÇÃO
Pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma decisão ou atividade da organização.

1. ESTABELECER o contexto
DESCRIÇÃO
- Identificar a influência do projeto/processo de TI avaliado nos objetivos estratégico e de tecnologia da informação, as partes interessadas, a legislação relacionada e a possível existência de listas de riscos, visando definir de forma clara o escopo da avaliação de riscos.
- Neste momento, deve ser elaborado também um diagrama do processo ou uma EAP do projeto em questão.
Adicionalmente, devem ser definidos os critérios de identificação, avaliação, tratamento e comunicação dos riscos, que serão utilizados ao longo do processo.
- Sempre que necessário, as partes interessadas no objeto da avaliação de riscos deverão ser consultadas/informadas.
- Todas as informações devem ser registradas no artefato D1 - Contexto da Gestão de Riscos, que será anexado, no sistema SEI, a processo específico para essa finalidade.

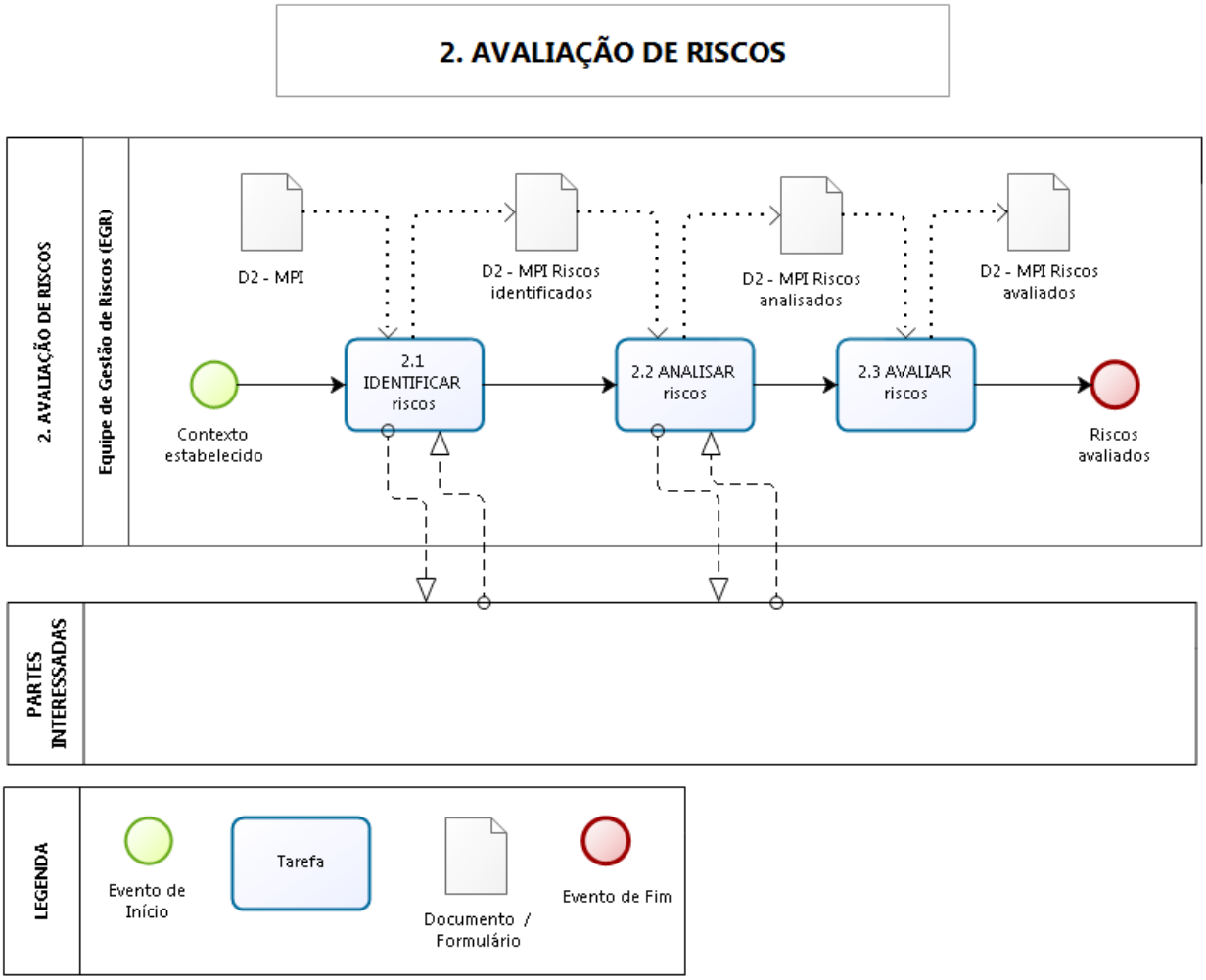
EXECUTANTE
Equipe de Gestão de Riscos (EGR)

D1 - Contexto da Gestão de Riscos
DESCRIÇÃO
D1 - Contexto da Gestão de Riscos
Onde é encontrado ou unidade responsável: ASPLAN-STI

2. AVALIAÇÃO DE RISCOS
Subprocesso

3. TRATAMENTO DE RISCO
Subprocesso

4. MONITORAMENTO E ANÁLISE CRÍTICA
Subprocesso Eventual


2. AVALIAÇÃO DE RISCOS
2. AVALIAÇÃO DE RISCOS
Equipe de Gestão de Riscos (EGR)
D2 - MPI
D2 - MPI Riscos identificados
D2 - MPI Riscos analisados
D2 - MPI Riscos avaliados
Contexto estabelecido
2.1 IDENTIFICAR riscos
2.2 ANALISAR riscos
2.3 AVALIAR riscos
Riscos avaliados
PARTES INTERESSADAS
LEGENDA
Evento de Início
Tarefa
Documento / Formulário
Evento de Fim

2.1 IDENTIFICAR riscos

DESCRIÇÃO

Identificar as fontes de risco, áreas de impactos, eventos (incluindo mudanças nas circunstâncias) e suas causas e consequências potenciais. A finalidade desta tarefa é gerar uma lista abrangente de riscos baseada nestes eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos do processo ou projeto sob análise.

EXECUTANTE

Equipe de Gestão de Riscos (EGR)

D2 - MPI

DESCRIÇÃO

D2 - Planilha Matriz de Probabilidade x Impacto (MPI)
Onde é encontrado ou unidade responsável: ASPLAN-STI

D2 - MPI Riscos identificados

DESCRIÇÃO

D2 - Planilha Matriz de Probabilidade x Impacto (MPI) - Riscos identificados

2.2 ANALISAR riscos

DESCRIÇÃO

- Identificar as causas e as fontes de risco, as consequências para o atingimento dos objetivos do processo/projeto, bem como a probabilidade de que essas consequências possam se concretizar, de acordo com os seguintes passos:
a) identificar, inicialmente, a categoria do risco, suas causas, consequências, bem como o impacto no atingimento dos objetivos, considerando o "Esforço de Gestão", a "Regulação", a "Reputação", os "Negócios" e a "Intervenção Hierárquica", calculando, ao final, o Nível de Risco Inerente (NRI);
b) baseado no passo anterior, identificar os controles preventivos e corretivos, para obtenção do Riscos de Controle (RC) e do Nível de Risco Residual (NRR);
c) categorizar o risco em "baixo", "médio", "alto" ou "muito alto".
- Utilizar o artefato D2- Planilha Matriz de Probabilidade x Impacto.

EXECUTANTE
Equipe de Gestão de Riscos (EGR)

D2 - MPI Riscos identificados
DESCRIÇÃO
D2 - Planilha Matriz de Probabilidade x Impacto (MPI) - Riscos identificados

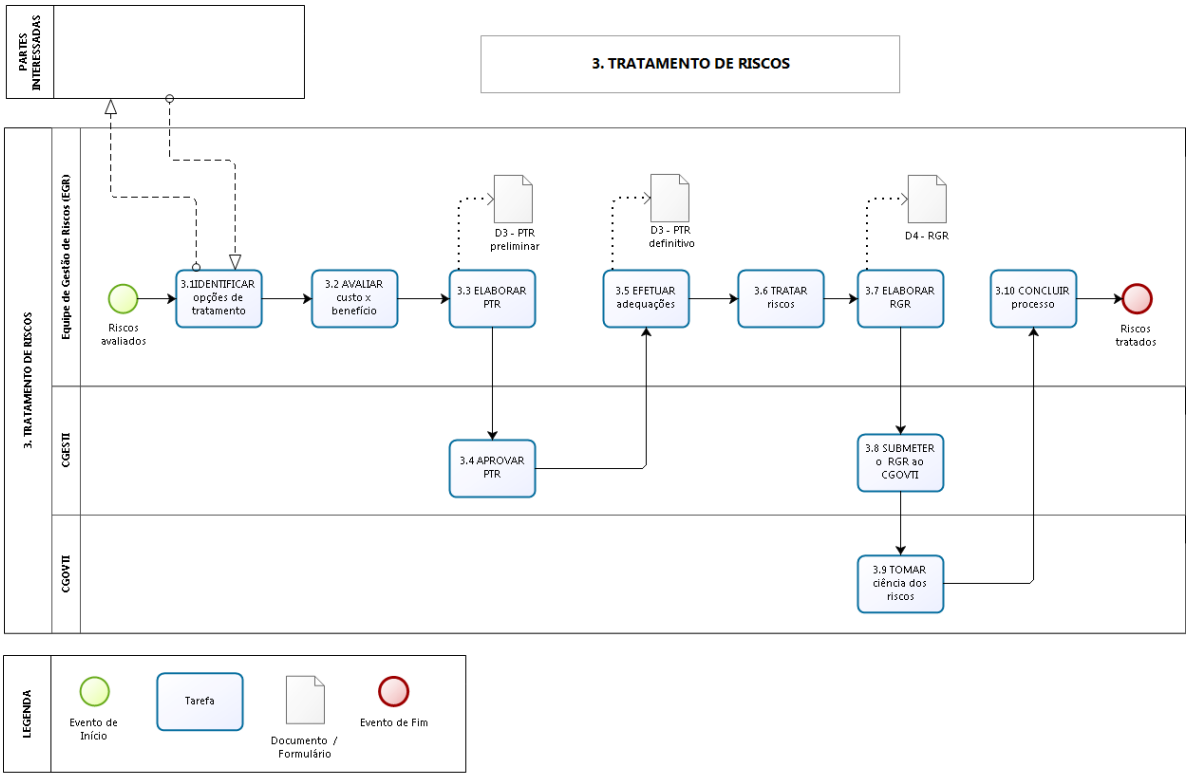
D2 - MPI Riscos analisados
DESCRIÇÃO
D2 - Planilha Matriz de Probabilidade x Impacto (MPI) - Riscos analisados

2.3 AVALIAR riscos
DESCRIÇÃO
- Comparar o nível de risco encontrado durante a etapa de análise com os critérios de risco estabelecidos quando o contexto foi considerado, visando subsidiar a decisão de tratamento dos riscos.
- Levar em conta a tolerância a riscos, os requisitos legais, regulatórios e outros requisitos.

EXECUTANTE
Equipe de Gestão de Riscos (EGR)

D2 - MPI Riscos analisados
DESCRIÇÃO
D2 - Planilha Matriz de Probabilidade x Impacto (MPI) - Riscos analisados

D2 - MPI Riscos avaliados
DESCRIÇÃO
D2 - Planilha Matriz de Probabilidade x Impacto (MPI) - Riscos avaliados


PARTES INTERESSADAS
3. TRATAMENTO DE RISCOS
3. TRATAMENTO DE RISCOS
Equipe de Gestão de Riscos (EGR)
CGESTI
CGOVTI
Riscos avaliados
3.1IDENTIFICAR opções de tratamento
3.2 AVALIAR custo x benefício
3.3 ELABORAR PTR
D3 - PTR preliminar
3.4 APROVAR PTR
3.5 EFETUAR adequações
D3 - PTR definitivo
3.6 TRATAR riscos
3.7 ELABORAR RGR
D4 - RGR
3.8 SUBMETER o RGR ao CGOVTI
3.9 TOMAR ciência dos riscos
3.10 CONCLUIR processo
Riscos tratados
LEGENDA
Evento de Início
Tarefa
Documento / Formulário
Evento de Fim

☐ 3.1 IDENTIFICAR opções de tratamento

DESCRIÇÃO

- Identificar as opções de tratamento dos riscos, considerando, inclusive, tratamentos de riscos que já foram realizados.
- As opções de tratamento a serem avaliadas são as seguintes:

a) **Evitar**: não iniciar ou descontinuar a atividade ou, ainda, desfazer-se do objeto sujeito ao risco;

b) **Reduzir ou mitigar**: adotar medidas para reduzir a probabilidade ou a consequência dos riscos ou até mesmo ambos;

c) **Compartilhar ou transferir**: é o caso especial de se mitigar a consequência ou probabilidade de ocorrência do risco por meio da transferência ou compartilhamento de uma parte do risco, mediante contratação de seguros ou terceirização de atividades nas quais a organização não tem suficiente domínio;

d) **Aceitar ou tolerar**: não tomar, deliberadamente , nenhuma medida para alterar a probabilidade ou a consequência do risco. Ocorre quando o risco está dentro do nível de tolerância da organização, a capacidade para fazer qualquer coisa sobre o risco é limitada ou, ainda, o custo de tomar qualquer medida é desproporcional em relação ao benefício potencial.

EXECUTANTE

Equipe de Gestão de Riscos (EGR)

☐ 3.2 AVALIAR custo x benefício

DESCRIÇÃO

Avaliar o equilíbrio entre os custos/esforços de implementação das medidas de mitigação do risco e os benefícios decorrentes,

EXECUTANTE

Equipe de Gestão de Riscos (EGR)

3.3 ELABORAR PTR

DESCRIÇÃO

Elaborar minuta do Plano de Tratamento de Riscos (PTR), que deve ser aprovado pelo Comitê de Gestão de TI (CGESTI).

EXECUTANTE

Equipe de Gestão de Riscos (EGR)

D3 - PTR preliminar

DESCRIÇÃO

D3 - Plano de Tratamento de Riscos (PTR) preliminar
Onde é encontrado ou unidade responsável: ASPLAN-STI

3.4 APROVAR PTR

DESCRIÇÃO

Avaliar a minuta do Plano de Tratamento de Riscos (PTR), sugerindo modificações quando necessário.

EXECUTANTE

Comitê de Gestão de TI (CGESTI)

3.5 EFETUAR adequações

DESCRIÇÃO

Efetuar as adequações necessárias, emitindo a versão final do documento.

EXECUTANTE

Equipe de Gestão de Riscos (EGR)

D3 - PTR definitivo

DESCRIÇÃO

D3 - Plano de Tratamento de Riscos (PTR) definitivo

3.6 TRATAR riscos

DESCRIÇÃO

Tratar os riscos conforme estratégia estabelecida no Plano de Tratamento de Riscos (PTR).

EXECUTANTE

Equipe de Gestão de Riscos (EGR)

3.7 ELABORAR RGR

DESCRIÇÃO

Elaborar o Relatório de Gestão de Riscos (RGR) com a consolidação da avaliação de riscos, submetendo-o para o Comitê de Gestão de TI (CGESTI).

EXECUTANTE

Equipe de Gestão de Riscos (EGR)

D4 - RGR

DESCRIÇÃO

D4 - Relatório de Gestão de Riscos
Onde é encontrado ou unidade responsável: ASPLAN-STI

3.8 SUBMETER o RGR ao CGOVTI

DESCRIÇÃO

Submeter o Relatório de Gestão de Riscos (RGR) para o conhecimento do Comitê de Governança de TI (CGOVTI), conforme a conveniência e a oportunidade.

EXECUTANTE

Comitê de Gestão de TI (CGESTI)

3.9 TOMAR ciência dos riscos

DESCRIÇÃO

Tomar ciência dos riscos de TI, emitindo recomendações, caso julgue necessário.

EXECUTANTE

Comitê de Governança de TI (CGOVTI)

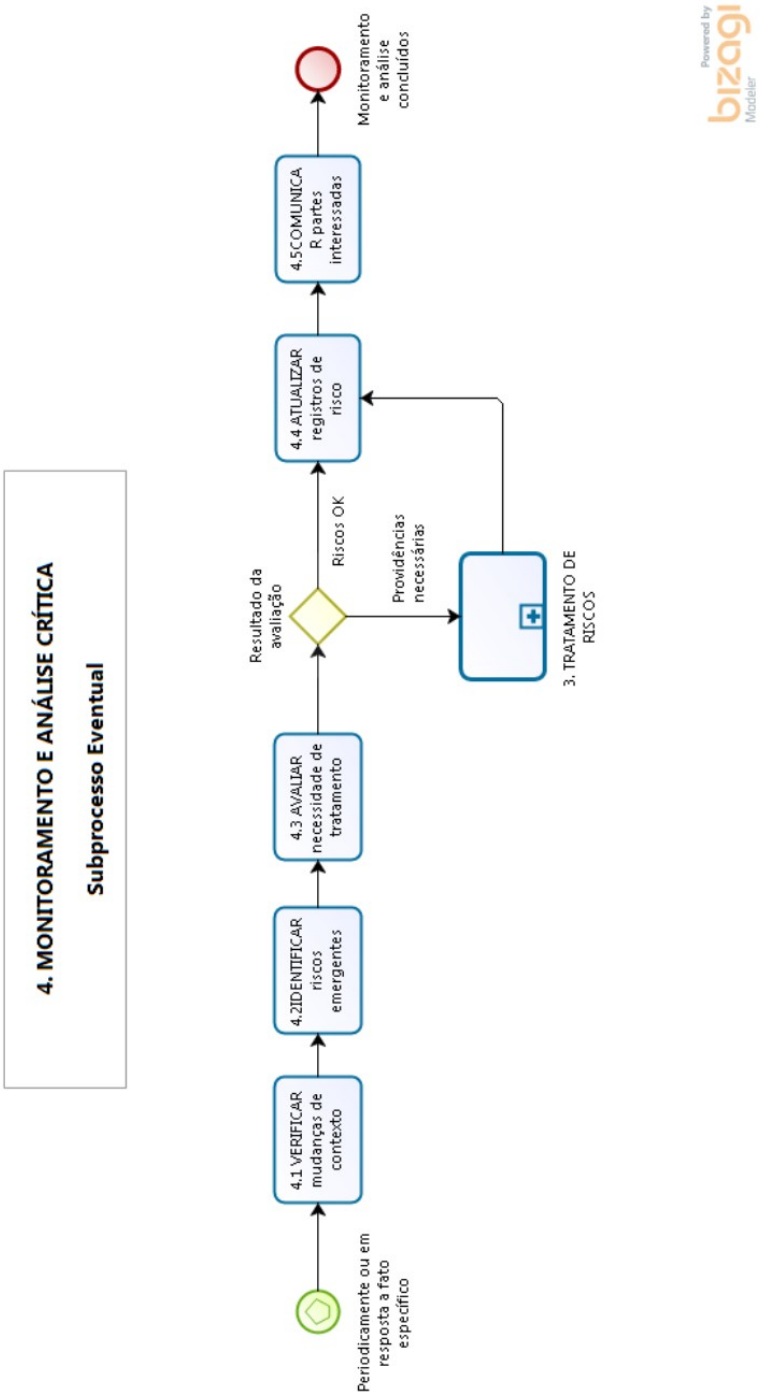
3.10 CONCLUIR processo

DESCRIÇÃO

Registrar os apontamentos necessários no processo SEI correspondente e desmobilizar a Equipe de Gestão de Riscos (EGR).

EXECUTANTE

Equipe de Gestão de Riscos (EGR)


4. MONITORAMENTO E ANÁLISE CRÍTICA
Subprocesso Eventual
Periodicamente ou em resposta a fato específico
4.1 VERIFICAR mudanças de contexto
4.2IDENTIFICAR riscos emergentes
4.3 AVALIAR necessidade de tratamento
Resultado da avaliação
Riscos OK
Providências necessárias
3. TRATAMENTO DE RISCOS
4.4 ATUALIZAR registros de risco
4.5COMUNICAR partes interessadas
Monitoramento e análise concluídos

☐ 4.1 VERIFICAR mudanças de contexto

DESCRIÇÃO

Verificar a ocorrência de mudanças nos contextos externo e interno, incluindo alterações nos critérios de risco e nos próprios riscos, visando adequar as medidas de tratamentos de riscos e suas prioridades.

EXECUTANTE

Gestor de Riscos

☐ 4.2 IDENTIFICAR riscos emergentes

DESCRIÇÃO

Identificar riscos novos ou riscos conhecidos cuja probabilidade de ocorrência ou grau de impacto tendem a aumentar.

EXECUTANTE

Gestor de Riscos

☐ 4.3 AVALIAR necessidade de tratamento

DESCRIÇÃO

- Com base nas informações coletadas nos passos anteriores, avaliar a necessidade de tratamento adicional dos riscos.
- Em caso afirmativo, encaminhar para a execução do subprocesso 3. TRATAMENTO DE RISCOS

EXECUTANTE

Gestor de Riscos

☐ 4.4 ATUALIZAR registros de risco

DESCRIÇÃO

- Registrar em processo específico as atividades de revisão e análise crítica, assim como as medidas de tratamento de riscos decorrentes da análise.

- Registro em: D1 - Contexto da Gestão de Riscos, D2 - Planilha Matriz de Probabilidade x Impacto, D3 - Plano de Tratamento de Riscos (PTR) ou D4 - Relatório de Gestão de Riscos (RGR), conforme o caso.

EXECUTANTE

Gestor de Riscos

☐ 4.5 COMUNICAR partes interessadas

DESCRIÇÃO

Comunicar às partes interessadas o resultado dos trabalhos.

EXECUTANTE

Gestor de Riscos