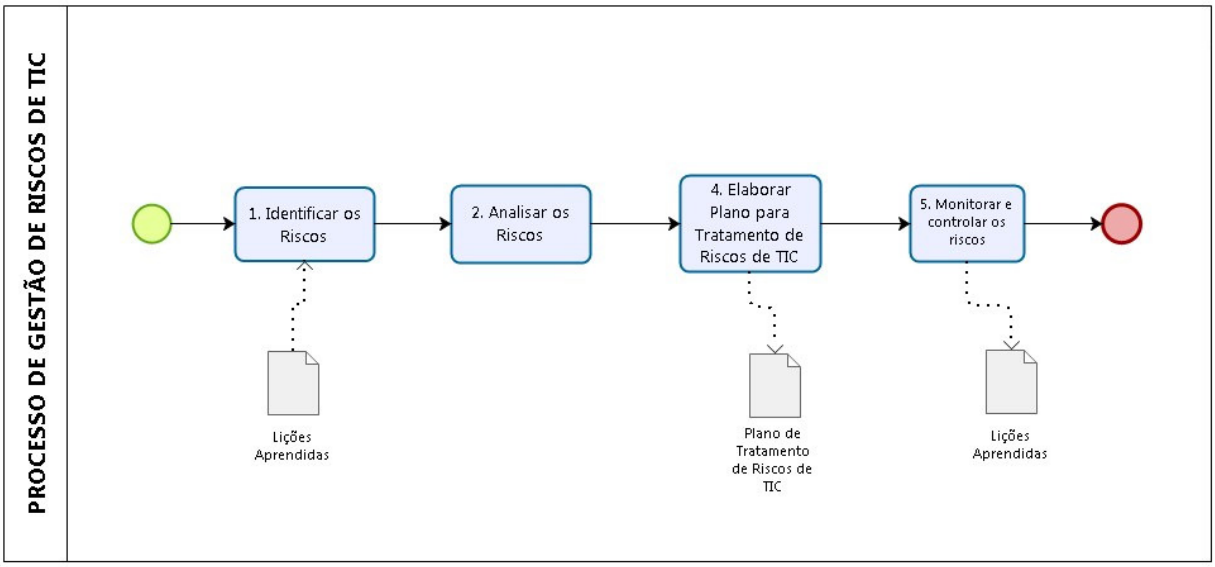
PODER JUDICIÁRIO FEDERAL
Justiça Eleitoral de Mato Grosso do Sul

Manual do Processo de Gestão de Riscos de Segurança da Informação

Agosto/2019

Índice

1 PROCESSO DE GESTÃO DE RISCOS DE TIC



1.1 PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Descrição

A necessidade de se gerenciar riscos de segurança da informação decorre, mormente, da consciência da existência de fatores internos ou externos ao processo de trabalho ou projeto, cujo desdobramento, pode vir a comprometer a integridade, a autenticidade, a confidencialidade, a disponibilidade e a irretratabilidade da informação.

Para realizar uma correta gestão de riscos de segurança da informação, é importante definir um responsável para identificar, analisar, avaliar, tratar, monitorar e comunicar o risco, denominado Gestor de Riscos. No âmbito deste Tribunal, o Gestor de Riscos será, via de regra, o dono do processo de trabalho ou o gerente de projeto.

Este documento detalha o Processo de Gestão de Riscos de Segurança da Informação, no âmbito deste Tribunal e tem por objetivo auxiliar os donos de processo de trabalho ou gerentes de projetos a reduzir a probabilidade de ocorrência e/ou o impacto de eventos negativos de segurança da informação.

O produto do presente Processo de Gestão de Riscos de Segurança da Informação, aplicado ao caso concreto, será um Plano para Tratamento de Riscos de Segurança da Informação, que será monitorado pelo respectivo Gestor de Riscos do processo de trabalho ou projeto pelo qual é responsável, durante sua execução.

Identificar os Riscos

Descrição

Identificar os eventos de riscos nos processos de trabalho ou projetos que podem afetar a segurança da informação, levando em consideração os fatores internos e externos do Tribunal.

O objetivo desta etapa é produzir uma lista de riscos de segurança da informação, que possam comprometer a integridade, a autenticidade, a confidencialidade, a disponibilidade e a irretratabilidade da informação. É de suma importância documentar os riscos, identificando claramente o que pode acontecer, bem como a forma como isso pode afetar o processo de trabalho ou projeto.

Essa identificação pode ser feita por meio de uma reunião, em que podem ser utilizadas técnicas e ferramentas como brainstorming, questionários, entrevistas com pessoas informadas ou especialistas, análise de dados históricos, técnica do grupo nominal, mapeamento de processos, entre outras. Convém que pessoas com conhecimento adequado sejam envolvidas na ação de identificação dos riscos.

Vale observar que o tipo de risco, a sua probabilidade de ocorrência, ou o seu impacto sobre o processo de trabalho ou projeto, variam ao longo do ciclo de vida do mesmo, sendo por isso necessário proceder-se à reavaliação dos riscos identificados.

Neste ponto do Processo de Gestão de Riscos de Segurança de Informação, é importante diferenciar “evento de risco” de “causa/fonte do risco”, um equívoco bastante comum entre os que lidam com essa matéria.

A primeira pergunta que se deve fazer é: “o que pode acontecer que afete de forma significativa o projeto ou o processo de trabalho?” Quando essa pergunta for respondida, teremos identificado o(s) “evento(s) de risco”. Para encontrar a causa/fonte correspondente, basta colocar outra pergunta: “o que pode causar esse risco?”. A resposta a essa pergunta, fornecerá a(s) causa(s)/fonte(s) do risco. Assim, podemos entender “evento de risco” como o próprio risco. E, partir daí, fica fácil entender que a causa/fonte do risco é aquilo que está associado a ele, que o motiva, que provoca o evento de risco. Essa distinção é importante porque, posteriormente, as ações de mitigação poderão ser implementadas naquilo que constitui a causa, a fonte do evento de risco.

Como dito acima, o mais importante no momento é distinguir o evento de risco das causas a ele associadas. Um bom exercício é fazer uma breve descrição do risco, abrangendo sua causa, o próprio evento de risco e sua consequência. Assim:

Devido a <CAUSA/FONTE>, poderá acontecer <DESCRIÇÃO DO EVENTO DE RISCO>, o que poderá levar a <DESCRIÇÃO DO IMPACTO/EFEITO/CONSEQUÊNCIAS>, comprometendo o <ASPECTO> de Segurança da Informação

#	Evento identificado	Causa/Fonte	Impacto ou efeito	Aspecto de SI
1	Usuário desligado do Tribunal, mas com login ativo	Falta de comunicação entre as unidades de RH e TI	Acesso indevido a informações internas	Confidencialidade

A tabela a seguir apresenta um rol não exaustivo de fatores internos e externos, que podem ser considerados na definição do cenário em que se insere o processo de trabalho ou o projeto em análise, para identificação dos eventos de risco que lhe dizem respeito.

Fatores Internos e Externos

FATORES INTERNOS	FATORES EXTERNOS
CONFORMIDADE E FISCALIZAÇÃO • Normatização, controle e fiscalização interna	REGULAMENTAÇÃO • Ambiente regulatório • Aderência aos principais requisitos regulatórios externos

GESTÃO DE PESSOAS • Carga de trabalho • Segregação de funções • Clima organizacional	FORNECEDORES • Relação com os fornecedores • Sanções ao contratado
TECNOLOGIA DA INFORMAÇÃO • Demanda interna por recursos de TI • Definição de parâmetros mínimos de qualidade e eficiência dos serviços prestados pela TI	DESASTRES • Inundação, incêndio e outros
CONTROLES FÍSICOS • 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 de governo
ECONÔMICOS • Disponibilidade financeiro-orçamentária	

Ao final desta etapa, estamos aptos a começar a pensar no que constituirá o resultado do Processo de Gestão dos Riscos de Segurança da Informação: o Plano para Tratamento dos Riscos de Segurança da Informação. Assim, com as informações levantadas até aqui, já temos alguns subsídios para preencher as primeiras colunas do Plano.

IDENTIFICAÇÃO DOS RISCOS				
	Evento de Risco	Causas/Fontes	Consequências	Aspecto de SI
1				

Analisar os Riscos

Descrição

Analisar os riscos identificados, definindo a probabilidade de sua materialização, bem como o impacto sobre os aspectos de segurança da informação do projeto ou processo de trabalho analisado, mediante a compreensão de sua natureza, do histórico de ocorrências, dos fatores temporais, da eficácia dos controles existentes, e da magnitude das consequências de sua ocorrência. Sabemos que todo risco tem, ao menos, uma causa ou fonte e, se ocorrer, pelo menos, um efeito ou consequência.

O propósito da análise de riscos é compreender a natureza dos riscos e suas características, estimando o nível de exposição que eles trazem ao processo de trabalho ou projeto. Um evento pode ter múltiplas causas e consequências e pode afetar múltiplos aspectos de segurança da informação.

Vale lembrar que a probabilidade está associada às chances de o evento ocorrer, ao passo que o impacto está associado às consequências do evento de risco ocorrido, ou seja, o resultado provável, no caso de o risco ocorrer.

Esta atividade pode ser realizada por meio de uma reunião de grupo, preferencialmente, com a mesma equipe que se reuniu para identificar os eventos de risco. A participação de especialistas externos à equipe é bem-vinda, principalmente se o órgão não tiver históricos de riscos de projetos anteriores, ou se a equipe não tiver experiência prévia com análise de riscos.

Ao definirmos a probabilidade, faremos uso das causas do risco levantadas na etapa anterior, e, para definirmos o impacto, olharemos para seus efeitos.

Sem o peso de cada risco, não temos como decidir adequadamente sobre que tipo de reação seria conveniente, ou quanto estaríamos dispostos a pagar para tratá-lo ou assumi-lo. De forma simplificada, se trabalharmos com valores numéricos para a probabilidade e o impacto, é possível fazer um simples cruzamento (multiplicação) entre esses valores e estimar nossa exposição ao risco, ou seja, o nível do risco, por meio de uma pontuação de probabilidade-impacto de cada risco, que implicará na obtenção de um percentual, que significará a chance de a causa do risco vir a ocorrer.

Tudo isso permitirá o estabelecimento de uma prioridade relativa de riscos individuais a serem avaliados em cada nível de prioridade.

Deverão ser consideradas as seguintes escalas de probabilidade e de impacto, levando em conta a existência de controles implementados que possam mitigá-los, bem como a eficácia desses controles.

ESCALA DE PROBABILIDADE (chances de um evento ocorrer)	
Muito baixa (1)	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade. Evento extraordinário, sem histórico de ocorrência.
Baixa (3)	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.

Média (5)	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade. Evento de frequência reduzida, e com histórico de ocorrência parcialmente conhecido.
Alta (7)	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade. Evento usual, com histórico de ocorrência amplamente conhecido.
Muito Alta (9)	Praticamente certa. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade. Evento repetitivo e constante.

ESCALA DE IMPACTO	
Muito baixo (1)	Impacto insignificante no processo de trabalho ou projeto.
Baixo (3)	Impacto mínimo no processo de trabalho ou projeto.
Médio (5)	Impacto moderado no processo de trabalho ou projeto, com possibilidade de recuperação.
Alto (7)	Impacto significativo no processo de trabalho ou projeto, com possibilidade remota de recuperação, de reversão.
Muito Alto (9)	Impacto máximo no processo de trabalho ou projeto, sem possibilidade de recuperação, ou seja, irreversível.

Com essas explicações, temos condições de calcular o nível do risco. Como o risco é uma função tanto da probabilidade, como da medida das consequências, seu nível pode ser expresso pela combinação da probabilidade de ocorrência do evento com as consequências resultantes no caso de materialização do evento, ou seja, do impacto nos aspectos de segurança da informação. A seguir, são apresentadas tabelas demonstrando, em valores numéricos e em categorias descritivas, o nível dos riscos para tomada de decisão quanto ao seu tratamento.

NÍVEL DE RISCOS

		Probabilidade				
		1 (Muito Baixa)	3 (Baixa)	5 (Média)	7 (Alta)	9 (Muito Alta)
Impacto	9 (Muito Alto)	9	27	45	63	81
	7 (Alto)	7	21	35	49	63
	5 (Médio)	5	15	25	35	45

	3 (Baixo)	3	9	15	21	27
	1 (Muito Baixo)	1	3	5	7	9

MATRIZ DE TOLERÂNCIA E CLASSIFICAÇÃO DE RISCOS

		Probabilidade				
		1 (Muito Baixa)	3 (Baixa)	5 (Média)	7 (Alta)	9 (Muito Alta)
Impacto	9 (Muito Alto)	9	27	45	63	81
	7 (Alto)	7	21	35	49	63
	5 (Médio)	5	15	25	35	45
	3 (Baixo)	3	9	15	21	27
	1 (Muito Baixo)	1	3	5	7	9

Risco Extremo/ Risco Inaceitável | Alto/ Risco Incaceitável | Médio/Aceitável Risco mediante análise Aceitável | Baixo/

A essa altura, já possuímos outras informações que serão incluídas no Plano para Tratamento dos Riscos de Segurança da Informação a ser finalizado na etapa “Elaborar Plano para Tratamento de Riscos de Segurança da Informação” adiante descrita.

ANÁLISE DOS RISCOS			
	Probabilidade	Impacto	Nível de Risco (Impacto x Probabilidade)
1			

Elaborar Plano para Tratamento de Riscos de Segurança da Informação

Descrição

Elaborar o Plano para Tratamento de Riscos de Segurança da Informação, com base nos resultados da análise realizada na etapa anterior.

Antes de finalizar o preenchimento do Plano para Tratamento de Riscos de Segurança da Informação, cujas informações preliminares já foram aferidas nas etapas anteriores, faz-se mister dedicarmos tempo a uma reflexão, para que a tomada de decisão com vistas à redução da exposição ao risco seja eficaz. Assim, com base nos resultados da análise de riscos já realizada, devemos pensar a) se um determinado risco precisa de tratamento e qual sua prioridade para isso; b) se uma determinada atividade deve ser realizada ou descontinuada; e c) se controles internos devem ser implementados ou, caso existam, se devem ser modificados, mantidos ou eliminados.

Esta é a hora de avaliar o nível de risco encontrado na etapa anterior à luz dos contextos externo e interno, com o intuito de determinar se o risco e/ou sua magnitude é aceitável ou tolerável, ou se algum tratamento é exigido.

A depender do contexto geral em que está inserido o projeto ou processo de trabalho e do nível dos riscos encontrados, o Gestor de Riscos deverá avaliar se está ao seu alcance decidir sobre as respostas a serem dadas no caso concreto. Pode ser que o nível do risco encontrado esteja acima de sua competência. Neste caso, o Gestor de Riscos encaminhará a questão para avaliação e decisão da Comissão de Segurança da Informação.

Sobre o tratamento dos riscos, há situações em que se requer uma ação sobre a probabilidade de ocorrência associada ao evento de risco. Outras vezes, ao planejarmos, pensamos em ações capazes de alterar o impacto de um evento de risco, caso ele ocorra. O desejável é que façamos as duas coisas – operemos tanto na probabilidade quanto no impacto associados ao evento de risco. Este é o momento de fazermos a seguinte reflexão: quanto custa tudo isso? Qual o custo-benefício do controle a ser implementado?

A elaboração propriamente dita do Plano para Tratamento de Riscos de Segurança da Informação correspondente a cada processo de trabalho ou projeto especificamente analisado, compreende o preenchimento das seguintes informações, além daquelas já coletadas nas etapas anteriores deste Processo de Gestão de Riscos:

a) os tipos de resposta (evitar; mitigar ou reduzir; compartilhar ou transferir; aceitar ou tolerar);
b) as ações de tratamento aos riscos;
c) o(s) responsável(is) pela implementação da ação;
d) as datas estimadas para a execução das ações de tratamento aos riscos, quer sejam riscos da alçada do próprio Gestor de Riscos ou não. Neste caso, deverão ser registradas as ações de tratamento deliberadas pelas autoridades competentes.

Gerir um risco compreende, basicamente, assumir uma das possíveis linhas de ação:

· Estabelecer ações de atenuação do risco, quer dizer, realizar ações para reduzir a probabilidade de sua materialização.

· Estabelecer ações de contingência, ou seja, realizar ações para se preparar diante da ocorrência do risco e reduzir o impacto que ele teria no projeto ou processo.

A seguir, elencamos os tipos de resposta possíveis de aplicação:

Evitar - objetiva descontinuar as atividades que geram o risco;

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. Antes de aceitar, 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.

A partir da seleção do tipo de resposta mais adequado, é que serão definidas efetivamente as ações de tratamento do risco. Nesta atividade, devem-se considerar alguns aspectos:

· Restrições organizacionais, técnicas e estruturais;

· Requisitos legais;

· Análise custo/benefício de cada resposta;

· Efeito de cada resposta sobre a probabilidade e o impacto; e

Prioridades.

Definidas as ações de tratamento dos riscos, é necessário proceder a nova avaliação de cada risco, de modo a se determinar o nível do risco residual, ou seja, aquele que eventualmente permanecerá, mesmo após a adoção das respostas planejadas; bem como o nível do(s) risco(s) secundário(s), assim compreendidos os que surgem como resultado direto da implantação de uma resposta ao risco. Assim, teremos novos níveis de risco, cuja necessidade de tratamento deverá ser avaliada.

Com as informações levantadas nesta etapa do Processo, estamos aptos a finalizar o preenchimento do Plano para Tratamento dos Riscos de Segurança da Informação (sugestão ao final do Manual), como a seguir:

#	Tipo de ação	Descrição das ações	Responsável pela implementação	Data do início	Data da conclusão	Risco Residual / Risco Secundário	Descrição de novas ações
1							

Monitorar e controlar os riscos

Descrição

Monitorar e controlar os riscos previstos no Plano para Tratamento de Riscos de Segurança da Informação.

Uma vez consolidado o Plano para Tratamento de Riscos de Segurança da Informação, o mesmo deverá ser monitorado pelo Gestor de Riscos. Durante o monitoramento, o Gestor de Riscos deverá manter atualizado um repositório de riscos e lições aprendidas, que poderá servir de referência na gestão de riscos de TIC de outros processos de trabalho ou projetos.

O principal benefício desta etapa é que ela possibilita que decisões relacionadas ao processo de trabalho ou projeto sejam tomadas com base em informações atuais sobre os riscos que os envolvem.

Vale ressaltar que o mero preenchimento do Plano para Tratamento de Riscos de Segurança da Informação não é suficiente para uma boa análise e gerenciamento de riscos. É preciso, a intervalos determinados, identificar novos riscos e testar a eficácia das medidas contidas no Plano para os riscos já previstos.

INDICADORES DE DESEMPENHO

É importante eleger e acompanhar indicadores de desempenho que possam demonstrar à alta administração e aos órgãos de controle interno e externo a garantia da eficácia do Processo de Gestão de Riscos de Segurança da Informação instituído e dos controles estabelecidos.

Assim, definimos os seguintes indicadores para medir a eficácia do Processo de Gestão de Riscos de Segurança da Informação estabelecido, sem prejuízo da apresentação de outros resultados que o Gestor de Riscos ou a Comissão de Segurança da Informação considerarem pertinentes para serem publicados.

A) Percentual de processos de trabalho em que foi implementado o Processo de Gestão de Riscos de Segurança da Informação.

Descrição: Mede o percentual de processos de trabalho com gestão de riscos de segurança da informação

Periodicidade: anualmente

Cálculo: nº de processos de trabalho com gestão de riscos de SI / nº total de processos de trabalho passíveis de gestão de riscos de SI

B) Percentual de Projetos em que foi implementado o Processo de Gestão de Riscos de Segurança da Informação.

Descrição: Mede o percentual de projetos com gestão de riscos de Segurança da Informação

Periodicidade: anualmente

Cálculo: nº de projetos em andamento com gestão de riscos de SI/ nº total de projetos em andamento passíveis de gestão de riscos de SI

RECURSOS

GESTORDERISCOS(FUNÇÃO)

Descrição

Donos de processo e gerentes de projeto com responsabilidade e autoridade para monitorar os riscos, bem como selecionar e implementar uma estratégia adequada de resposta a risco.

PLANO PARA TRATAMENTO DE RISCOS DE TIC													
IDENTIFICAÇÃO DOS RISCOS				ANÁLISE DOS RISCOS			PLANEJAMENTO DAS AÇÕES DE TRATAMENTO						
#	Evento de Risco	Causa/Fonte	Consequências	Probabilidade	Impacto	Nível de Risco (Probabilidade x Impacto)	Tipo de Ação	Descrição das ações	Responsável pela implementação	Data do início	Data da conclusão	Risco residual / risco secundário	Descrição de novas ações