RISCOS DE TIC

Processos de TIC

Data: 28/06/2019

Versão 1.2

DEPARTAMENTO DE
TECNOLOGIA DA INFORMAÇÃO
E COMUNICAÇÃO

Brasil. Tribunal de Justiça do Estado do Paraná. Departamento de Tecnologia da Informação e Comunicação.

Documentação de Processos de TIC / Tribunal de Justiça do Estado do Paraná, Departamento de Tecnologia da Informação e Comunicação. - Curitiba: TJPR, 2017. 16 p.: il.

1. Tecnologia da informação. 2. Gestão pública. 3. Administração Pública. 4. Gestão e Governança. 5. Processos de TI.

HISTÓRICO DE ALTERAÇÕES

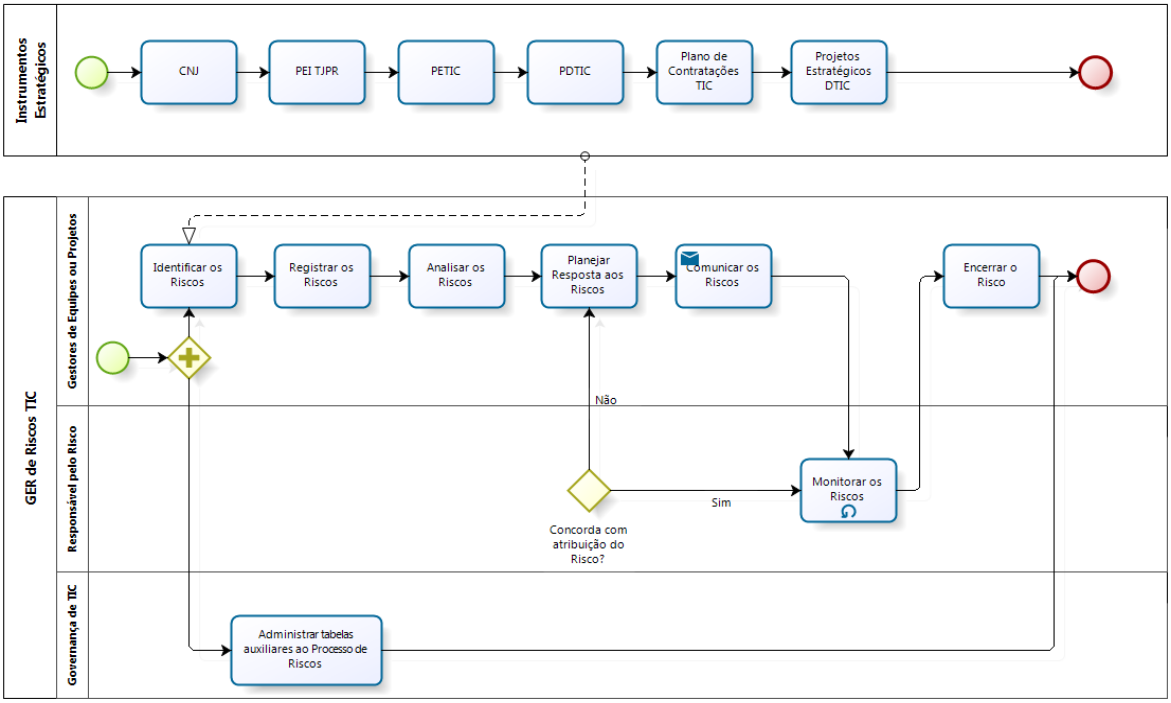
DOCUMENTO			
Descrição	Documento de Processo de TIC para o fluxo de Gerenciamento de Riscos de TIC no DTIC.		
Objetivo	Este documento descreve as atividades e procedimentos adotados para o Gerenciamento de Riscos de TIC no DTIC do TJPR.		
Responsável	Pablo Tavares	**Divisão**	Assessoria Técnica
Criado em	15/02/2017	**Revisão**	Anual

VERSIONAMENTOS			
Versão	Data	Autor	Descrição
1.0	15/02/2017	Equipe Governança de TIC	Criação e Revisão do Documento
1.1	07/02/2019	Equipe Governança de TIC	Atualização da Cúpula Diretiva
1.2	28/06/2019	Equipe Governança de TIC	Atualizado Logotipo TJPR conforme Resolução TJPR 227/2019

Sumário

1. GERENCIAR RISCOS DE TIC

1.1. Diagrama do Processo



1.2. Descrição das Atividades

1.2.1. Identificar os Riscos

Objetivo:

- Levantar os prováveis riscos que podem afetar o negócio, a execução de projetos de TIC, e documentar suas características.

Entradas:

- Atas de reunião sobre levantamento dos riscos.

Descrição das Atividades:

- Identificar a maior quantidade possível de eventos ou situações no ambiente do projeto que possam impacta-lo futuramente;
- Reuniões de brainstorm;
- Envolver a equipe do projeto e stakeholders do projeto;
- Nesta atividade definir no mínimo:

I. Causa;

II. Nome/Título do Risco;

III. Efeito do risco (as consequências, caso o risco aconteça);

IV. Categoria do Risco: Os riscos foram identificados e agrupados em categorias, com vistas a facilitar seu gerenciamento. Segue algumas sugestões de categorias:

- Estratégicos: Estão associados à tomada de decisão que pode afetar negativamente o alcance dos objetivos da organização.

- Operacional: Riscos que afetam o desempenho e a qualidade das atividades operacionais de TI. Os riscos devem ser mitigados, transferidos, eliminados ou explorados, pois não poderão ser aceitos.

- Reputação ou Imagem: Riscos que podem afetar a imagem do DTIC ou da organização. Os riscos devem ser mitigados, transferidos, eliminados ou explorados, pois não poderão ser aceitos.

- Financeiro: Estão associados ao não cumprimento de princípios constitucionais, legislações específicas ou regulamentações externas aplicáveis ao negócio, bem como de normas e procedimentos internos.

- Conformidade: Riscos externos ao controle direto do TJPR, mas que ainda assim podem afetar o sucesso das metas e ação (dependência de outras áreas do TJPR / CNJ, reestruturação organizacional, suporte organizacional, mudanças no governo, mercado e tecnologias etc.). Os riscos externos podem ser aceitos, pois independem de ação direta do Ibama.

- Tecnologias: Riscos relacionados a problemas técnicos em hardware, software ou outra solução de informática (apontamento genérico).

- Infraestrutura de TI: Riscos relacionados a problemas técnicos em hardware, software, ou demais equipamentos de TI (exige conhecimento técnico para definir esta categoria).

- Software: Riscos relacionados a problemas técnicos em um software específico (exige conhecimento técnico para definir esta categoria).

- Escopo: Riscos relacionados ao assunto escopo de um projeto, exemplo: indefinições, alterações constantes, sem validação.

- Cliente / Usuário: Riscos relacionados a clientes ou usuários de algum projeto, por exemplo: indefinição, representante ausente, sem comprometimento.

V. Tipo do Risco: pode ser positivo (Oportunidade) ou negativo (Ameaça);

Saídas:

- Lista de Riscos Identificados.

1.2.2. Registrar os Riscos

Objetivo:

- Catalogar todos os riscos discutidos na atividade anterior.

Entradas:

- Lista de Riscos identificados.

Descrição das Atividades:

- Registrar a lista de riscos para o conhecimento geral dos demais envolvidos no projeto, e demais participantes da organização.

Saídas:

- Central de Riscos de TIC atualizada.

1.2.3. Analisar os Riscos

Objetivo:

- Avaliar a probabilidade de ocorrência e o impacto causado pelos riscos identificados.

Entradas:

- Lista de Riscos catalogados na Central de Riscos de TIC.

Descrição das Atividades:

- Avaliar em cada risco:

a) Qual a probabilidade de ocorrência baseado em (estimativa) do risco.

A probabilidade e o impacto são variáveis independentes. Geralmente, usa-se uma escala entre três a cinco pontos para parametrizar as estimativas dos eventos (ameaças ou oportunidades). Aconselha-se a utilizar uma escala não linear, a fim de dar maior peso a eventos com alta probabilidade, em detrimento de eventos com baixa probabilidade.

Escala de Probabilidade de Riscos				
Risco	**Baixa**	**Moderada**	**Alta**	**Muito Alta**
Peso	1	3	6	10

b) Qual a gravidade do impacto ou efeitos ou consequências do impacto baseado em (estimativa).

A concretização de um determinado evento produz impactos que no âmbito do gerenciamento de riscos no DTIC foram classificados qualitativamente em quatro (04) níveis:

Escala de Impacto Negativo do Risco				
Sobre o objetivo do projeto	**Insignificante (1)**	**Moderado (3)**	**Relevante (6)**	**Catastrófico (10)**
Sobre os custos	Aumento de até 5%	Aumento de 5,01% até 10%	Aumento de 10,01% até 20%	Aumento acima de 20,01%
Sobre o cronograma	Atraso de até 5%	Atraso de 5,01% até 10%	Atraso de 10,01% até 30%	Atraso acima de 30,01%
Sobre o escopo	Redução imperceptível	Partes pouco importantes afetadas	Sistemas críticos afetados	Produto final não serve para o cliente
Sobre a qualidade	Degradação imperceptível	Degradação de itens não prioritários	Degradação de qualidade significativa	Produto final sem uso

c) calcular a criticidade, ou seja, o produto da probabilidade versus impacto.

Deve-se observar que cada assunto abordado pelo riso pode ser necessário adotar um parâmetro ou uma escala diferente, por exemplo, um impacto Alto para cronograma é quando existe possibilidade de atrasar entre 10,01% a 30%, já para o assunto escopo, o impacto Alto é quando os sistemas críticos são afetados. Multiplicam-se os valores atribuídos para a PROBABILIDADE pelo valor do IMPACTO, ou seja: **Criticidade do Risco = Probabilidade X Impacto**

FÓRMULA PARA CALCULAR A CRITICIDADE DO RISCO:				
PROBABILIDADE	**CRITICIDADE (ameaças)**			
Muito Alta (10)	**10**	**30**	**60**	**100**
Alta (6)	**6**	**18**	**36**	**60**
Moderada (3)	**3**	**9**	**18**	**30**
Baixa (1)	**1**	**3**	**6**	**10**
IMPACTO =>	**Insignificante (1)**	**Moderado (3)**	**Relevante (6)**	**Catastrófico (10)**

Saídas:

- Central de riscos de TIC com criticidade calculada.

1.2.4. Planejar Resposta aos Riscos

Objetivo:

- Definir estratégias de respostas aos riscos, ou seja, execução de um plano ou conjunto de medidas adequadas de redução do risco, com base no processo de avaliação.

Entradas:

- Lista de Riscos catalogados na Central de Riscos de TIC.

Descrição das Atividades:

- Definir em cada risco, o tipo de tratamento, ou seja, qual será a estratégia de resposta ao risco a ser adotada:

  a) Prevenir ou Evitar: quando o risco é elevado em termos de impacto e probabilidade, simplesmente não pode ser aceito. Deve-se planejar uma forma de eliminá-lo completamente; mudar o plano do projeto, não iniciar ou descontinuar a atividade que dá origem ao risco. Exemplo: adotar uma abordagem tradicional em vez de uma inovadora; excluir do escopo a área sujeita a risco. Nesse caso, o plano do projeto será necessariamente alterado. Se não for possível alterar o plano do projeto, a opção será a transferência do risco. (37 a 100 pontos de criticidade);

  b) Transferir ou Compartilhar: se o risco é inaceitável, porém não há como alterar o planejamento do projeto, procura-se tranferir o impacto negativo e a responsabilidade da resposta terceirizando as etapas do trabalho afetadas pelo risco. Indicado repassar as consequências do risco bem como a responsabilidade de resposta para quem está mais bem-preparado para enfrentá-lo. Exemplo: contratos com fornecedor contendo cláusulas específicas para tratamento dos riscos. (37 a 100 pontos de criticidade);

  c) Mitigar (suavizar) ou reduzir: desenvolver ações visando minimizar a probabilidade da ocorrência ou de seu impacto, com o objetivo de deixar

o risco dentro do limite aceitável. Exemplo: projetar uma redundância; qualificação de recursos humanos. (11 a 36 pontos de criticidade);

d) Aceitar: indicada nas situações em que a criticidade do risco é Moderado ou Insignificante; ou na ocorrência de riscos externos em que não seja possível implementar uma ação específica. Existem algumas derivações:

- Aceitar **passivamente o risco**: simplesmente não fazer nada e torcer para que o risco não venha a acontecer; ou prever que o risco exigirá resposta, mas não será preciso reservar recursos adicionais (01 a 03 pontos de criticidade);
- Aceitar **ativamente o risco**: desenvolver planos alternativos (Contingência) caso venha a ocorrer. Neste caso será necessário alocação de valores monetários (04 a 10 pontos de criticidade).

Resumidamente, conforme tabela abaixo:

Criticidade	**Baixo**	**Moderado**	**Elevado**	**Extremo**
	1 a 3	4 a 10	11 a 36	37 a 100
Resposta ao Risco	**Aceitar Passivamente**	**Aceitar Ativamente**	**Mitigar / Reduzir**	**Prevenir/Evitar ou Transferir/Compartilhar**

- Ação Redutora: descrever ações que devem ser realizadas em função do tipo de tratamento / estratégia adotada;

- Ação Corretiva / Contingência: definir um plano de ação ou conjunto de atividades para atuar caso o risco aconteça efetivamente;

- Definição do Responsável pela Correção: definir o responsável ou equipe (s) que deve (m) ser acionada (s);

- Gatilho: situação que pode acionar o risco (data, hora ou evento?) Se é hora de acionar a contingência (o risco ocorreu?);

- Envolvidos: representantes que devem acompanhar / comunicar os riscos (nome / área / contatos);

- Tempo Limite do Risco: indicar quando o risco deixa de ser representativo ou válido (data e hora) que o mesmo deve ser descartado;

- Nível de Visibilidade: visível somente para a área interna da TI ou ao cliente também;

- Status do Risco: situação atual do risco. Opções:

    1. Ativo: risco ainda pode ocorrer;

    2. Ocorrido: tornou-se um “problema”;

    3. Cancelado: risco foi desconsiderado após análise;

    4. Obsoleto: não há mais possibilidade de ocorrer, geralmente a fase do projeto onde ele iria acontecer já terminou;

    5. Pausa: o risco não será monitorado por enquanto;

    6. Fechado: o risco foi resolvido com sucesso.

Saídas:

- Central de riscos de TIC com plano de resposta aos riscos.

1.2.5. Comunicar os Riscos

Objetivo:

- Compartilhar continuamente as informações referentes aos riscos entre as partes interessadas durante todo o processo de gestão de risco.

Entradas:

- Lista de Riscos catalogados na Central de Riscos de TIC.

Descrição das Atividades:

- Definir um plano de comunicação, ou no mínimo a periodicidade e forma de divulgação dos riscos de TIC aos envolvidos.

Saídas:

- Lista de Riscos a serem comunicados.

1.2.6. Monitorar os Riscos

Objetivo:

- Manter atualizado as informações dos riscos da Central de Riscos de TIC.

Entradas:

- Lista de Riscos catalogados na Central de Riscos de TIC.
- Sistemas de relatórios internos e externos (disclosure);
- Auditorias internas;
- Estabelecimento de técnicas de medição (ex. V@R, simulações de Monte Carlo etc.);
- Balanced Scorecard adaptado.

Descrição das Atividades:

- Definir uma periodicidade para atualização das informações dos riscos;
- Avaliar validade do risco perante o cenário atual;
- Atualizar os status do risco.

Saídas:

- Central de riscos de TIC com as informações atualizadas.

1.2.7. Encerrar o Risco

Objetivo:

- Encerrar o (s) risco (s) que já foram monitorados ou se tornaram obsoletos para o monitoramento.

Entradas:

- Central de riscos de TIC com as informações atualizadas.

Descrição das Atividades:

- Definir o critério para encerramento do risco:

  a) Riscos obsoletos;

  b) Riscos que aconteceram, e não precisam ser considerados novamente;

  c) Riscos que aconteceram, e podem ser recorrentes;

  d) Riscos cancelados pelo solicitante;

- Registrar a justificativa do encerramento do risco;

- Comunicar aos envolvidos sobre o encerramento do risco;

- Comunicar o Comitê gestor TIC e Comitê Segurança TIC quando o risco é cancelado ou deletado.

Saídas:

- Risco encerrado, com justificativa;
- Comunicação aos envolvidos;
- Central de riscos de TIC com as informações atualizadas.

1.2.8. Administrar tabelas auxiliares ao Processo de Riscos

Objetivo:

- Cadastrar e Atualizar informações administrativas ou de apoio sobre os riscos.

Entradas:

- Definições sobre o Processo de Gestão de Riscos.

Descrição das Atividades:

- Cadastrar as informações básicas sobre os riscos;
- Atualizar as informações básicas sobre os riscos.

Saídas:

- Central de riscos de TIC com as informações atualizadas.