**TRIBUNAL REGIONAL ELEITORAL**
**RIO GRANDE DO NORTE**

# Manual do Processo
# Gestão Corporativa de Riscos de TIC

---

**VERSÃO 1.0**

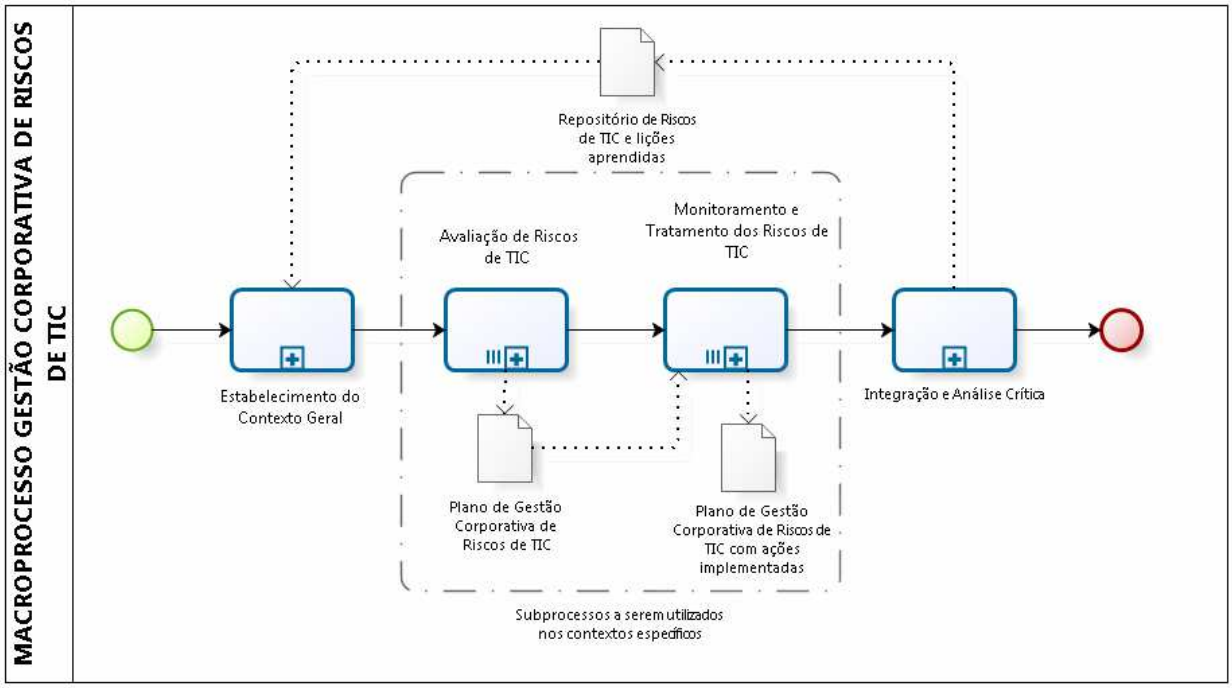
Natal
Agosto/2016

## CONTROLE DE VERSÕES

| DATA | VERSÃO | ALTERAÇÃO | RESPONSÁVEL |
|---|---|---|---|
| AGOSTO/2016 | 1.0 | Versão inicial (adaptação do material produzido pelo Grupo Governança de TIC – Justiça Eleitoral) | Gabinete e Apoio a Planejamento e Gestão/STIC |

# ÍNDICE

# 1 MACROPROCESSO GESTÃO CORPORATIVA DE RISCOS DE TIC



# 1.1 MACROPROCESSO GESTÃO CORPORATIVA DE RISCOS DE TIC

## 1.1.1 ELEMENTOS DO PROCESSO

### 1.1.1.1  Estabelecimento do Contexto Geral

**Descrição**

Este Subprocesso visa ao estabelecimento do ambiente de gerenciamento corporativo de riscos de TIC (contexto geral), e identifica os fatores internos e externos, bem como os critérios de riscos (escalas de probabilidade e impacto; a relação entre elas; apetite a riscos e matriz de classificação dos riscos) que servirão como subsídio para o estabelecimento dos contextos específicos de cada caso concreto (projeto, processo, contratação ou outro) que será instanciado.

Em princípio, trata-se de um processo que deve ser realizado uma única vez, devendo ser alterado sempre que necessário, nas Reuniões de Análise Estratégica (RAEs).

### 1.1.1.2  Avaliação de Riscos de TIC

**Descrição**

Este Subprocesso tem por objetivo avaliar os riscos do projeto, processo, contratação ou outro, a partir do levantamento do contexto específico em que o caso concreto está inserido, até a elaboração do respectivo Plano de Gestão Corporativa de Riscos de TIC (Anexo).

### 1.1.1.3  Monitoramento e Tratamento dos Riscos de TIC

**Descrição**

Este Subprocesso constitui um controle interno, onde se verifica a ocorrência do risco e a efetividade do Plano de Gestão Corporativa de Riscos de TIC (Anexo), em especial, da "resposta ao risco" nele contida.

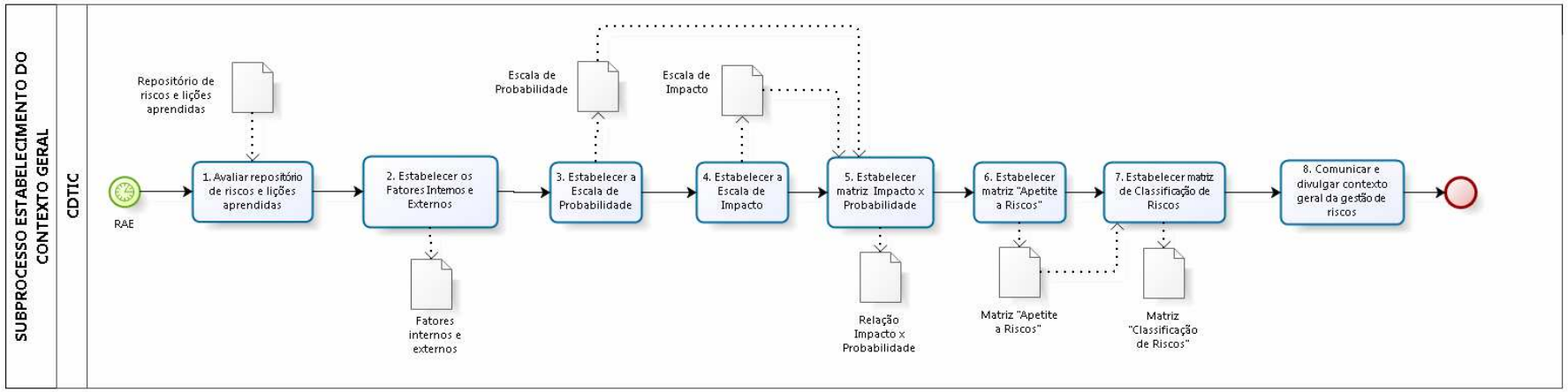
Neste caso, o foco é a prevenção de cada risco e também resolução de cada evento de risco que se torna realidade. Entretanto, pelo fato de os controles internos serem normalmente específicos para cada tipo de risco, conclui-se que, resolvendo um risco (preventiva ou corretivamente), validam-se os respectivos controles internos.

#### 1.1.1.4  Integração e Análise Crítica

**Descrição**

Este Subprocesso visa à integração dos Planos de Gestão Corporativa de Riscos de TIC em um Repositório de Riscos de TIC que contenha as Lições Aprendidas em cada Processo, Projeto, Contratação ou outro que for instanciado.

# 2 ESTABELECIMENTO DO CONTEXTO GERAL



# 2.1 SUBPROCESSO ESTABELECIMENTO DO CONTEXTO GERAL

## 2.1.1 ELEMENTOS DO PROCESSO

### 2.1.1.1 1. Avaliar repositório de riscos e lições aprendidas

**Descrição**

Avaliar relatório de Lições Aprendidas e *Repositório de Riscos de TIC* , que é repassado ao CETIC pela unidade de apoio à Governança de TIC, a título de compilação de todos os Planos de Gestão Corporativa de Riscos de TIC.

**Executante**

CDTIC

### 2.1.1.2 2. Estabelecer os Fatores Internos e Externos

**Descrição**

Estabelecer os fatores internos e externos que, em conjunto com os critérios de riscos, formarão o ambiente de gerenciamento corporativo de riscos de TIC (contexto geral).

A Tabela 1 apresenta um rol não exaustivo de categorias de eventos a serem consideradas na definição do CONTEXTO GERAL da organização.

**Executante**

CDTIC

**Tabela 1: Fatores Internos e Externos**

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

**Executante**

CDTIC

### 2.1.1.3 3. Estabelecer a Escala de Probabilidade

**Descrição**

Estabelecer a(s) Escala(s) de Probabilidade que será(ão) utilizada(s) como base para aplicação ao caso concreto.

Os critérios de riscos compreendem as escalas de probabilidade e impacto, a relação entre elas, bem como a matriz de classificação dos riscos (nível e apetite).

A tabela 2 apresenta um modelo de escala de probabilidade que define as chances de o evento ocorrer. O Proprietário de Risco poderá adequar somente os quantitativos da coluna "ocorrências", a depender do caso concreto.

A escala de probabilidade abaixo demonstrada pode variar de "muito baixa", "baixa", "média", "alta" a "muito alta".

**Tabela 2: Escala de Probabilidade**

| ESCALA DE PROBABILIDADE | | | |
|---|---|---|---|
| **DESCRITOR** | **DESCRIÇÃO** | **OCORRÊNCIAS** | **NÍVEL** |
| Muito Baixa | Evento extraordinário, sem histórico de ocorrência. | Até 5 | 1 |
| Baixa | Evento casual e inesperado, sem histórico de ocorrência. | > 5 Até 10 | 2 |
| Média | Evento esperado, de frequência reduzida, e com histórico de ocorrência parcialmente conhecido. | > 10 Até 15 | 3 |
| Alta | Evento usual, com histórico de ocorrência amplamente conhecido. | > 15 Até 20 | 4 |
| Muito Alta | Evento repetitivo e constante. | > 20 | 5 |

**Executante**

CDTIC

### 2.1.1.4 4. Estabelecer a Escala de Impacto

**Descrição**

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:

**Tabela 3: Impacto nas Dimensões do Objetivo**

| 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", "baixo", "médio", "alto" a "muito alto".

Nem sempre o nível será o mesmo para todas as dimensões. Caso isso aconteça, considerar-se-á como o nível de impacto o mais alto encontrado, para a sua classificação, conforme a seguir:

**Tabela 4: Escala de Impacto**

| 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 |

**Executante**

CDTIC

### 2.1.1.5 5. Estabelecer matriz Impacto x Probabilidade

**Descrição**

Estabelecer matriz Impacto x Probabilidade, a partir da relação dos níveis de probabilidade e impacto, definindo-se, assim, o Nível de Risco (valor numérico), conforme tabela a seguir:

**Tabela 5: Matriz Impacto x Probabilidade**

| LEGENDA NÍVEL DE RISCO<br>EXTREMO<br>ALTO<br>MÉDIO<br>BAIXO | | PROBABILIDADE | | | | |
|---|---|---|---|---|---|---|
| | | 1<br>Muita Baixa | 2<br>Baixa | 3<br>Média | 4<br>Alta | 5<br>Muito Alta |
| IMPACTO | 5<br>Muito Alto | 5 | 10 | 15 | 20 | 25 |
| | 4<br>Alto | 4 | 8 | 12 | 16 | 20 |
| | 3<br>Médio | 3 | 6 | 9 | 12 | 15 |
| | 2<br>Baixo | 2 | 4 | 6 | 8 | 10 |
| | 1<br>Muito Baixo | 1 | 2 | 3 | 4 | 5 |

**Executante**

CDTIC

### 2.1.1.6 6. Estabelecer matriz "Apetite a Riscos"

**Descrição**

Estabelecer a Matriz "Apetite a Riscos" do Tribunal, a partir do nível de risco (valor numérico) encontrado, podendo variar conforme o perfil da instituição (mais ou menos conservador) e o caso concreto, de "oportunidade", "aceitável", "inaceitável" a "absolutamente inaceitável", de acordo com a tabela a seguir:

**Executante**

CDTIC

Tabela 6: Matriz "Apetite a Riscos"

| LEGENDA NÍVEL DE RISCO<br>EXTREMO<br>ALTO<br>MÉDIO<br>BAIXO | | PROBABILIDADE | | | | |
|---|---|---|---|---|---|---|
| | | 1<br>Muita Baixa | 2<br>Baixa | 3<br>Média | 4<br>Alta | 5<br>Muito Alta |
| IMPACTO | 5<br>Muito Alto | | | | ABSOLUTAMENTE INACEITÁVEL | |
| | 4<br>Alto | | | | | |
| | 3<br>Médio | | | INACEITÁVEL | | |
| | 2<br>Baixo | | ACEITÁVEL | | | |
| | 1<br>Muito Baixo | OPORTUNIDADE | | | | |

**Executante**

CDTIC

### 2.1.1.7 7. Estabelecer matriz de Classificação de Riscos

**Descrição**

Estabelecer Matriz de Classificação de Riscos, através da tabela abaixo que, necessariamente, constituirá um "espelho" da tabela anterior de apetite a risco, podendo variar de "baixo", "médio", "alto" a "extremo".

Tabela 7: Matriz de Classificação de Riscos

| LEGENDA NÍVEL DE RISCO<br>EXTREMO<br>ALTO<br>MÉDIO<br>BAIXO | | PROBABILIDADE | | | | |
|---|---|---|---|---|---|---|
| | | 1<br>Muita Baixa | 2<br>Baixa | 3<br>Média | 4<br>Alta | 5<br>Muito Alta |
| IMPACTO | 5<br>Muito Alto | | | EXTREMO | | |
| | 4<br>Alto | | | | | |
| | 3<br>Médio | | | ALTO | | |
| | 2<br>Baixo | BAIXO | MÉDIO | | | |
| | 1<br>Muito Baixo | | | | | |

**Executante**

CDTIC

### 2.1.1.8 8. Comunicar e divulgar contexto geral da gestão de riscos

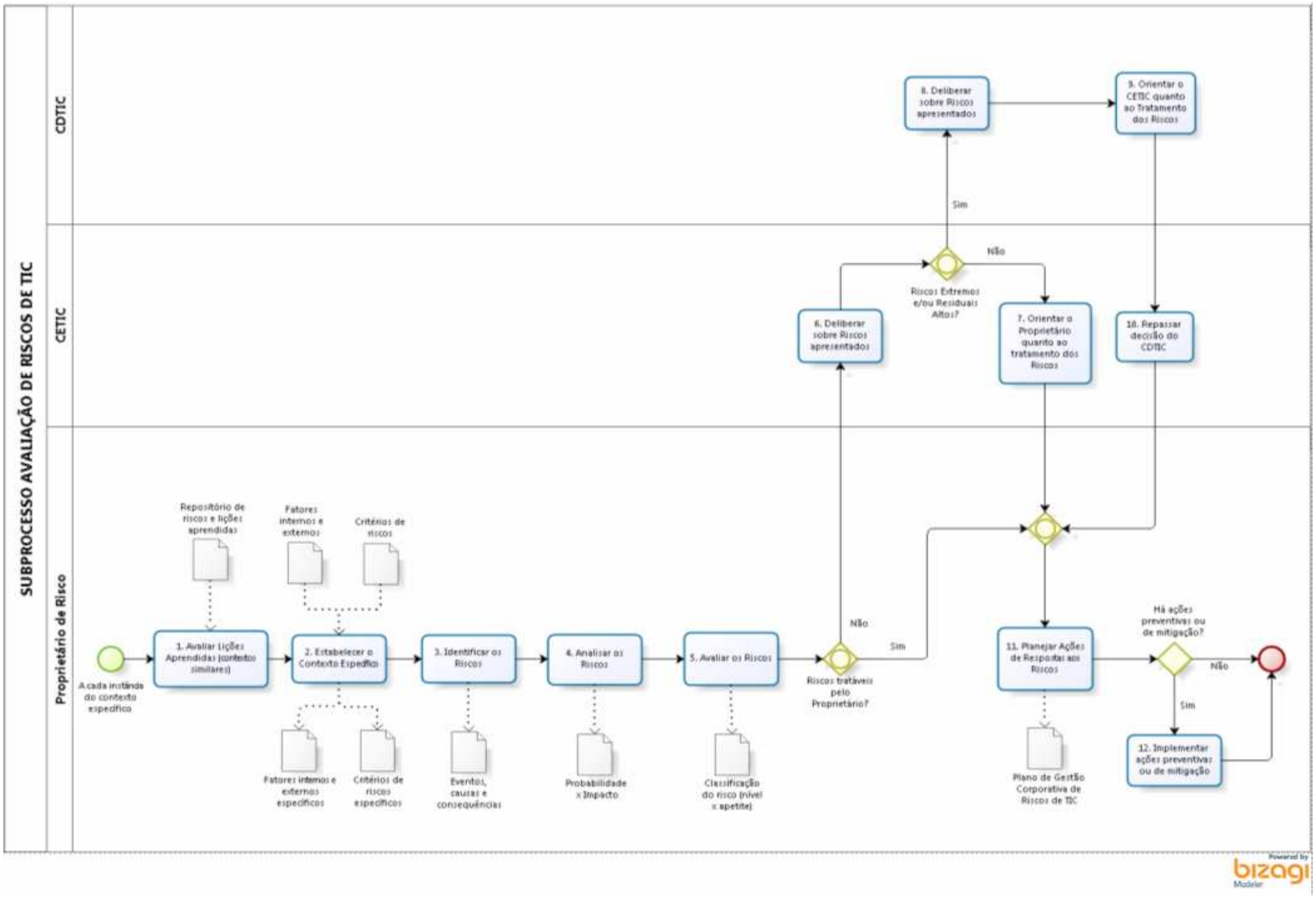
**Descrição**

Publicar na *intranet* e *internet* o material balizador da Gestão Corporativa de Riscos de TIC do Tribunal: Política de Gestão Corporativa de Riscos de TIC, Modelagem do Processo Corporativo de Gestão de Riscos de TIC, Manual do Processo de Gestão Corporativa de Riscos de TIC e Modelo de Plano de Gestão Corporativa de Riscos de TIC (Anexo). Promover, sempre que necessário, reuniões de sensibilização no tema, treinamentos, entre outros. Deve-se sempre observar o Plano de Comunicação do processo, projeto ou outro que for instanciado.

**Executante**

CDTIC

# 3 AVALIAÇÃO DE RISCOS DE TIC

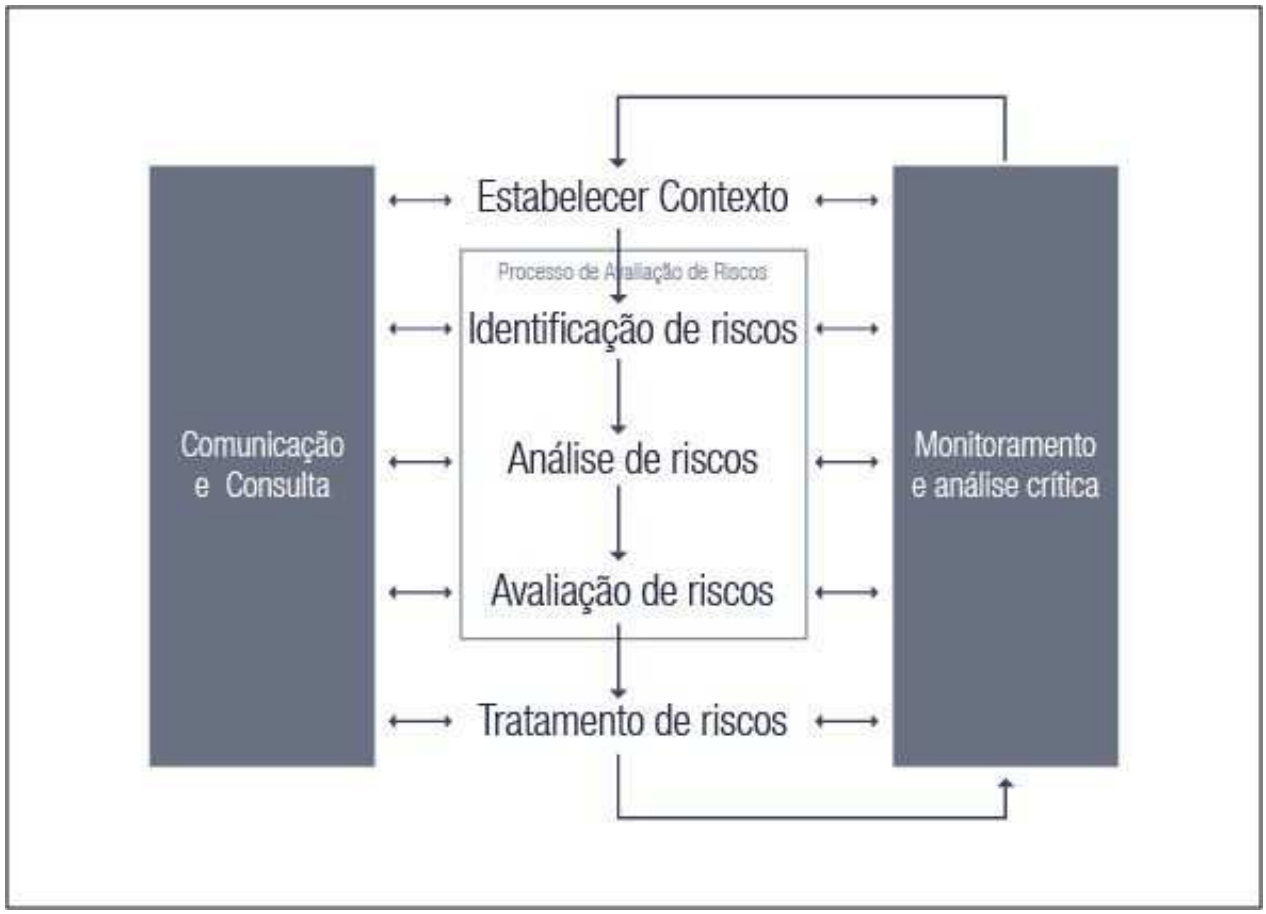


## 3.1 SUBPROCESSO AVALIAÇÃO DE RISCOS DE TIC

**Descrição**

Este documento tem por objetivo detalhar o Processo de Gestão de Riscos previsto na Política Corporativa de Gestão de Riscos de Tecnologia da Informação e Comunicação da Secretaria do Tribunal, instituída por meio da Resolução TRE/RN nº XX/2016, a fim de auxiliar sua implantação.

Eis o processo de Gestão de Riscos, de acordo com a ABNT NBR ISO 31.000:2009:



## 3.1.1 ELEMENTOS DO PROCESSO

### 3.1.1.1 1. Avaliar Lições Aprendidas (contextos similares)

**Descrição**

Avaliar Lições Aprendidas de contextos similares, quando houver, como subsídio para estabelecimento do Contexto Específico.

**Executante**

Proprietário de Risco

### 3.1.1.2 2. Estabelecer o Contexto Específico

**Descrição**

Identificar, com base no Contexto Geral estabelecido, os fatores externos e internos que devem ser levados em consideração para gerenciar os riscos no caso concreto (CONTEXTO ESPECÍFICO), seja em processo, projeto, contratação ou outro.

Dessa forma, o Proprietário de Risco deverá ajustar as categorias de eventos discriminadas na Tabela 1 (Fatores Internos e Externos) resultante do Subprocesso Estabelecimento do Contexto Geral, excluindo as que não se aplicam ao caso concreto, e incluindo as que não estiverem previstas.

Eventualmente, o Proprietário de Risco adaptará os critérios de riscos definidos na Tabela 2 (Escala de Probabilidade) e na Tabela 3 (Impacto nas Dimensões do Objetivo), conforme orientado no Subprocesso Estabelecimento do Contexto Geral.

Nesta atividade, havendo mais de uma Matriz de Classificação de Riscos estabelecida pela Instituição, o proprietário de risco deverá eleger a que será aplicada ao caso concreto.

**Executante**

Proprietário de Risco

### 3.1.1.3 3. Identificar os Riscos

**Descrição**

Identificar os riscos que podem influenciar os objetivos estabelecidos, indicando os eventos, as respectivas causas e consequências. A título de ilustração, apresenta-se o exemplo a seguir:

**Tabela 8: Exemplo de Identificação de Riscos (parte integrante do Plano de Gestão Corporativa de Riscos de TIC)**

| | | | | |
|---|---|---|---|---|
| **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** | | | | |

Para esta atividade, podem ser utilizadas técnicas e ferramentas como *brainstorming*, questionários, entrevistas, análise de dados históricos, entre outros.

A seguir, apresentam-se algumas sugestões de categoria e eventos de riscos baseadas no *framework* COSO II:

**Tabela 9: Exemplo de Eventos por Categoria de Riscos**

| CATEGORIA | ESTRATÉGICO | OPERACIONAIS | DE COMUNICAÇÃO | DE CONFORMIDADE |
|---|---|---|---|---|
| **EVENTOS** | Erros de tomada de decisão da alta administração, decorrentes da má gestão ou de definições externas, que podem afetar negativamente o alcance dos objetivos institucionais (tendo como foco o processo eleitoral, a segurança da informação, a continuidade dos serviços essenciais de TIC), visão estratégica mal compreendida, plano estratégico não definido ou desatualizado, estrutura organizacional inapropriada, falta de integração entre processos organizacionais, partes interessadas não identificadas, falta de apoio da Alta Administração, ausênicia do Plano de Continuidade do Negócio. | Ocorrência de perdas (produtividade, ativos, recursos humanos, orçamentos, dentre outros) resultantes de falhas; de deficiências ou inadequação de processos internos, de estrutura, de pessoas, de sistemas e de tecnologia; assim como de eventos externos (catástrofes naturais, greves, fraudes, dentre outros), requisitos de Segurança da Informação não definidos, falta de integração dos Sistemas de TIC, ausência do controle de acesso aos Sistemas de TIC, obsolescência dos sistemas de TIC, sistemas de TIC não escalonáveis, falhas nos projetos de TIC, bem como responsáveis por atividades operacionais não definidos, falta de execução dos testes do plano de recuperação de desastres, funções e responsabilidades não segregadas. | Eventos que podem impedir ou dificultar a disponibilidade de informações para a tomada de decisões e para o cumprimento das obrigações de prestação de contas às instâncias controladoras e à sociedade (*accountability*); riscos de abalo na credibilidade do processso eleitoral, da morosidade da justiça eleitoral, vazamento de informações sigilosas (dados do cadastro de eleitor), transparência dos dados públicos. | Não cumprimento de princípios constitucionais, legislações específicas ou regulamentações externas aplicáveis ao negócio, bem como de normas e procedimentos internos; ausência de legislação interna, desconformidade com a legislação externa, existência de cláusulas contratuais exorbitantes, mudanças nos requisitos de entrega dos serviços, entrega dos serviços em desconformidade com os requisitos, ingerência das relações com fornecedores. |

O resultado desta atividade deverá ser registrado no Plano de Gestão Corporativa de Riscos de TIC (Anexo).

Por ocasião do Subprocesso Monitoramento e Tratamento dos Riscos de TIC, caso seja identificado um risco novo, o Plano de Gestão Corporativa de Riscos de TIC deverá ser atualizado com os novos riscos identificados. Neste caso, deverá seguir com o Subprocesso Avaliação de Riscos a partir desta atividade (Identificar os Riscos), até o Planejamento das Ações de Respostas aos Riscos, atualizando o Plano de Gestão Corporativa de Riscos de TIC existente, confome Processo de Gestão Corporativa de Riscos de TIC desenhado.

Em qualquer caso, não se deve deixar de registrar o risco ainda não acontecido, sob pena de não se estar preparado para sua ocorrência. Também pode ser preciso disparar ações de mitigação do risco (ações preventivas, a serem executadas antes da ocorrência do risco). Assim, em geral, uma vez identificado novo risco ainda não mapeado, deve-se registrá-lo e planejar a resposta a ele, seja preventiva ou corretiva.

**Executante**

Proprietário de Risco

#### 3.1.1.4  4. Analisar os Riscos

**Descrição**

Definir os níveis de probabilidade e de impacto do risco, mediante a compreensão de sua natureza, do histórico de ocorrências, e do impacto nas dimensões "custo", "prazo", "escopo" e "qualidade" do objetivo pretendido.

Para tanto, deverão ser consideradas as escalas de probabilidade e de impacto definidas anteriormente (no Subprocesso Estabelecimento do Contexto Geral, Atividades 3 e 4).

Aplicando as definições acima ao caso exemplificado na atividade anterior (Evento de risco: Provimento do pedido de impugnação do edital), tem-se a tabela a seguir para a definição do nível de probabilidade do risco:

**Tabela 10: Exemplo de uso da Tabela Escala de Probabilidade**

| DESCRITOR | DESCRIÇÃO DA PROBABILIDADE | OCORRÊNCIAS | NÍVEL |
|---|---|---|---|
| Alta | Evento usual, com histórico de ocorrência amplamente conhecido | > 15 Até 20 | **4** |

Para definir o nível de impacto, **recomenda-se, primeiramente,** avaliar quais dimensões (custo, prazo, escopo e qualidade) do objetivo do caso concreto serão influenciadas direta ou indiretamente na provável ocorrência do evento.

Nesse sentido, aplicando-se a Tabela 3 (Impacto nas Dimensões do Objetivo) ao caso hipotético em estudo, tem-se:

**Tabela 11: Exemplo de uso da Tabela Impacto nas Dimensões do Objetivo**

| IMPACTO NAS DIMENSÕES DO OBJETIVO | | | | |
|---|---|---|---|---|
| **CUSTO ( aumento % )** | **PRAZO (atraso %)** | **ESCOPO (afetação)** | **QUALIDADE (degradação)** | **NÍVEL** |
| Até 5 | | Insignificante | Irrisória | |
| | | | | |
| | | | | |
| | | | | |
| | >20 | | | **5** |

Conforme salientado no Subprocesso Estabelecimento do Contexto Geral, nem sempre o nível de impacto nas dimensões será o mesmo para todas elas. Caso isso aconteça, considerar-se-á como nível de impacto no objetivo o mais alto encontrado.

Percebe-se que, no preenchimento da Tabela 11 acima, considerou-se que:

a. O custo não sofrerá variação na hipótese do risco de impugnação se materializar;

b. O prazo sofrerá forte atraso, estimado em mais de 20%, pois o termo de referência será revisto;

c. O escopo, que para este exemplo é o termo de referência, não será afetado;

d. A qualidade do objetivo também não será afetada.

Assim, em resumo, as dimensões "Custo", "Escopo" e "Qualidade" alcançaram níveis de impacto baixos. No entanto, como a dimensão "Prazo" alcançou o mais alto nível (5), esse será o valor considerado para Nível de Impacto no objetivo, conforme tabela a seguir:

**Tabela 12: Exemplo de Uso da Tabela Escala de Impacto**

| DESCRITOR | DESCRIÇÃO | NÍVEL |
|---|---|---|
| MUITO ALTO | Impacto máximo nos objetivos sem possibilidade de recuperação | **5** |

No caso em estudo, pela descrição do Nível de Impacto da Tabela 12 acima, é possível afirmar que, se o Termo de Referência não for revisto, certamente o objetivo do processo de trabalho não será atendido (Elaborar o Termo de Referência necessário à contratação, em conformidade com a legislação vigente).

### Executante

Proprietário de Risco

### 3.1.1.5 5. Avaliar os Riscos

**Descrição**

Relacionar os resultados aferidos na atividade anterior, para posterior classificação do risco com base no apetite definido.

Para que o Nível do Risco seja definido, os níveis de probabilidade e de impacto devem ser relacionados:

*Nível de Probabilidade (4) x Nível de Impacto (5) = Nível do Risco (20)*

O resultado desse relacionamento encontra-se na tabela a seguir:

**Tabela 13: Exemplo de Uso da Tabela Matriz Impacto x Probabilidade**

| LEGENDA NÍVEL DE RISCO<br>EXTREMO<br>ALTO<br>MÉDIO<br>BAIXO | | PROBABILIDADE | | | | |
|---|---|---|---|---|---|---|
| | | | | | 4<br>Alta | |
| IMPACTO | 5<br>Muito Alto | | | | 20 | |

No processo de trabalho em foco (Evento de risco: Provimento do pedido de impugnação do edital), após a definição do nível de risco (valor numérico = 20), e com base na Matriz de Apetite a Risco eleita para o caso, depreende-se que se trata de um risco "absolutamente inaceitável", conforme tabela a seguir:

**Tabela 14: Exemplo de Uso da Tabela Matriz "Apetite a Riscos"**

| LEGENDA NÍVEL DE RISCO<br>EXTREMO<br>ALTO<br>MÉDIO<br>BAIXO | | PROBABILIDADE | | | | |
|---|---|---|---|---|---|---|
| | | | | | 4<br>Alta | |
| IMPACTO | 5<br>Muito Alto | | | | ABSOLUTAMENTE INACEITÁVEL | |

Finalmente, o Proprietário de Risco estará apto a classificar o risco, utilizando a Matriz de Classificação de Riscos definida pelo órgão para aquele cenário específico (Estabelecimento dos Contextos Geral e Específico). No caso em apreço, o risco será classificado como "extremo", conforme demonstrado a seguir:

**Tabela 15: Exemplo de Uso da Tabela Matriz de Classificação de Riscos**

| **LEGENDA NÍVEL DE RISCO**<br>**EXTREMO**<br>**ALTO**<br>**MÉDIO**<br>**BAIXO** | | **PROBABILIDADE** | | | | |
|---|---|---|---|---|---|---|
| | | | | | **4**<br>**Alta** | |
| **IMPACTO** | **5**<br>**Muito Alto** | | | | **EXTREMO (20)** | |

Depois de avaliados os riscos, com base no apetite a risco definido pela instituição para o caso concreto, será verificada a existência de controles implementados que possam mitigá-los, bem como a eficácia desses controles, utilizando-se a tabela a seguir:

**Tabela 16: Definição da 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 |

Dessa avaliação de controles, o Proprietário de Risco obterá um índice (Risco de Controle), que será multiplicado pelo Nível de Risco encontrado, a fim de obter o **risco residual**, conforme exemplo a seguir:

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **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** | **Probabilidade** | **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 |

É com base no risco residual que serão planejadas as ações preventivas ou de mitigação. O resultado desta atividade deverá ser registrado no Plano de Gestão Corporativa de Riscos de TIC (Anexo).

### Executante

Proprietário de Risco

#### 3.1.1.6 6. Deliberar sobre Riscos apresentados

**Descrição**

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.

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.

**Executante**

CETIC

#### 3.1.1.7 7. Orientar o Proprietário quanto ao tratamento dos Riscos

**Descrição**

Orientar o Proprietário de Risco quanto às ações a serem implementadas, deliberadas pelo CETIC.

**Executante**

CETIC

#### 3.1.1.8 8. Deliberar sobre Riscos apresentados

**Descrição**

Analisar todos os riscos extremos e residuais altos reportados pelo CETIC, cujo estabelecimento das ações de tratamento estiver acima da competência e autoridade daquele Comitê Executivo.

Esta atividade deverá tomar por base a avaliação técnica e propostas de ações apresentadas pelo CETIC.

**Executante**

CDTIC

#### 3.1.1.9 9. Orientar o CETIC quanto ao Tratamento dos Riscos

**Descrição**

Orientar o CETIC quanto às ações a serem implementadas, deliberadas pelo CDTIC.

**Executante**

CDTIC

#### 3.1.1.10 10. Repassar decisão do CDTIC

**Descrição**

Repassar ao Proprietário de Risco as orientações fornecidas pelo CDTIC, quanto às ações a serem implementadas.

**Executante**

CETIC

#### 3.1.1.11 11. Planejar Ações de Respostas aos Riscos

**Descrição**

Registrar no Plano de Gestão Corporativa de Riscos de TIC (Anexo) os tipos de resposta, ações de tratamento aos riscos e, ainda, responsáveis e 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).

A seguir, os tipos de resposta possíveis de aplicação:

**RISCOS NEGATIVOS**

**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 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.

**RISCOS POSITIVOS**

**Explorar** - objetiva eliminar a incerteza associada a um determinado risco positivo, garantindo que a oportunidade realmente aconteça;

**Melhorar** - objetiva aumentar a probabilidade e/ou os impactos positivos de uma oportunidade;

**Compartilhar** - objetiva alocar integral ou parcialmente a responsabilidade da oportunidade a um terceiro que tenha mais capacidade de explorá-la para benefício do projeto, processo, contratação ou outro;

**Aceitar** - objetiva aproveitar uma oportunidade, caso ela ocorra, mas não persegui-la ativamente.

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:

- Eficácia das ações já existentes
- Restrições organizacionais, técnicas e estruturais
- Requisitos legais
- Análise custo/benefício de cada resposta
- Efeito de cada resposta sobre a probabilidade e o impacto
- Prioridades

O resultado desta atividade, assim como as informações relacionadas nas atividades de identificação, análise e avaliação de riscos, serão consolidados no Plano Gestão Corporativa de Riscos de TIC (Anexo).

Uma vez consolidado o Plano de Gestão Corporativa 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, conforme desenho do processo.

**Executante**

Proprietário de Risco

#### 3.1.1.12 12. Implementar ações preventivas ou de mitigação

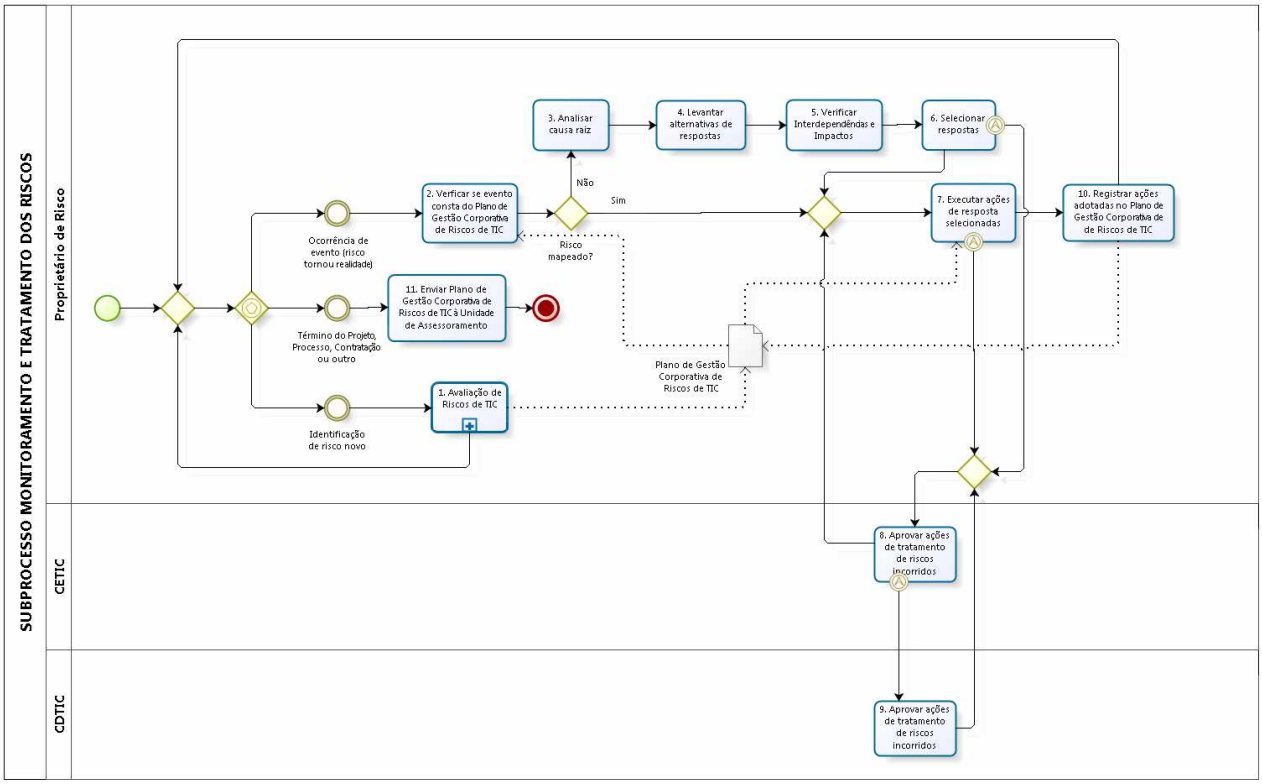
**Descrição**

Implementar eventuais ações preventivas ou de mitigação dos riscos previstas no Plano de Gestão Corporativa de Riscos de TIC.

**Executante**

Proprietário de Risco

# 4 MONITORAMENTO E TRATAMENTO DOS RISCOS DE TIC



# 4.1 SUBPROCESSO MONITORAMENTO E TRATAMENTO DOS RISCOS

## 4.1.1 ELEMENTOS DO PROCESSO

### 4.1.1.1 1. Avaliação de Riscos de TIC

**Descrição**

Caso seja identificado um risco novo, o Plano de Gestão Corporativa de Riscos de TIC deverá ser atualizado com o(s) novo(s) risco(s) identificado(s). Neste caso, deverá seguir com o Subprocesso Avaliação de Riscos a partir da atividade Identificar os Riscos, até o Planejamento das Ações de Respostas aos Riscos, atualizando o Plano de Gestão Corporativa de Riscos de TIC existente, conforme Processo de Gestão Corporativa de Riscos de TIC desenhado.

Em qualquer caso, não se deve deixar de registrar o risco ainda não acontecido, sob pena de não se estar preparado para sua ocorrência. Também pode ser preciso disparar ações de mitigação do risco (ações preventivas, a serem executadas antes da ocorrência do risco). Assim, em geral, uma vez identificado novo risco ainda não mapeado, deve-se registrá-lo e planejar a resposta a ele, seja preventiva ou corretiva.

**Executante**

Proprietário de Risco

### 4.1.1.2 2. Verificar se evento consta do Plano de Gestão Corporativa de Riscos de TIC

**Descrição**

No caso de um evento de risco tornar-se realidade, verificar se o risco que se tornou realidade já foi mapeado no Plano de Gestão Corporativa de Riscos de TIC e, se for o caso, disparar as ações planejadas. Se não mapeado, proceder à análise do Risco, identificando sua causa raiz e o impacto gerado.

**Executante**

Proprietário de Risco

#### 4.1.1.3 3. Analisar causa raiz

**Descrição**

Analisar causa raiz do evento (origem).
O ponto de partida para a proposição de ações eficazes é o conhecimento das causas últimas do evento. Se a causa raiz não for identificada, corre-se o risco de tratar o sintoma sem resolver a questão.

**Executante**

Proprietário de Risco

#### 4.1.1.4 4. Levantar alternativas de respostas

**Descrição**

Levantar alternativas de respostas ao evento, uma vez analisadas a(s) causa(s) raíz(es), para implementá-las ou submetê-las à instância de decisão competente.

**Executante**

Proprietário de Risco

#### 4.1.1.5 5. Verificar Interdependências e Impactos

**Descrição**

Verificar interdependência do evento em relação às alternativas de respostas levantadas, e avaliar seus impactos, antes e depois de implementadas as ações de respostas.

As relações de dependência entre as alternativas de solução levantadas e o impacto gerado pelo evento devem ser explicitadas para fundamentar a escolha da resposta ao risco.

**Executante**

Proprietário de Risco

#### 4.1.1.6 6. Selecionar respostas

**Descrição**

Selecionar ações de resposta ao evento, dentre as alternativas levantadas.

A proposição de ações deve indicar as providências a serem tomadas para tratar o evento de risco acontecido. Se necessário, escalar as ações propostas para autorização superior (CETIC ou CDTIC), antes de executá-las, conforme Política Corporativa de Gestão de Riscos de TIC estabelecida.

Após definição das ações de resposta, atualizar Plano de Gestão Corporativa de Riscos de TIC existente (Anexo).

**Executante**

Proprietário de Risco

#### 4.1.1.7 7. Executar ações de resposta selecionadas

**Descrição**

Executar as ações de resposta ao evento selecionadas, caso estejam na alçada de decisão do Proprietário de Risco. Caso não estejam, observar se já foram deliberadas pelos entes competentes (CETIC ou CDTIC), conforme Política Corporativa de Gestão de Riscos de TIC. Em qualquer caso, tais ações devem estar previamente descritas no Plano de Gestão Corporativa de Riscos de TIC atualizado.

**Executante**

Proprietário de Risco

#### 4.1.1.8 8. Aprovar ações de tratamento de riscos incorridos

**Descrição**

Aprovar ações não previamente autorizadas, de acordo com seu nível de autonomia. Se necessário, escalar para decisão superior (CDTIC).

Caso as ações de resposta a risco de sua competência tenham sido implementadas, tomar ciência de sua execução através de relatório do Proprietário de Risco.

**Executante**

CETIC

#### 4.1.1.9 9. Aprovar ações de tratamento de riscos incorridos

**Descrição**

Aprovar ações não previamente autorizadas, de acordo com sua competência.

Caso as ações de resposta a risco de sua competência tenham sido implementadas, tomar ciência de sua execução através de relatório do Proprietário de Risco encaminhado ao CETIC.

**Executante**

CDTIC

#### 4.1.1.10 10. Registrar ações adotadas no Plano de Gestão Corporativa de Riscos de TIC

**Descrição**

Registrar no Plano de Gestão Corporativa de Riscos de TIC as ações que foram implementadas após ocorrido o evento de risco, bem como os resultados obtidos e as lições aprendidas.

Após registro no Plano de Gestão Corporativa de Riscos de TIC, reportá-lo à unidade de apoio à Governança de TIC ou equivalente, para fins de integração, monitoramento e reporte ao CETIC, quando necessário, conforme atividade a seguir.

**Executante**

Proprietário de Risco

#### 4.1.1.11 11. Enviar Plano de Gestão Corporativa de Riscos de TIC à Unidade de Apoio à Governança de TIC

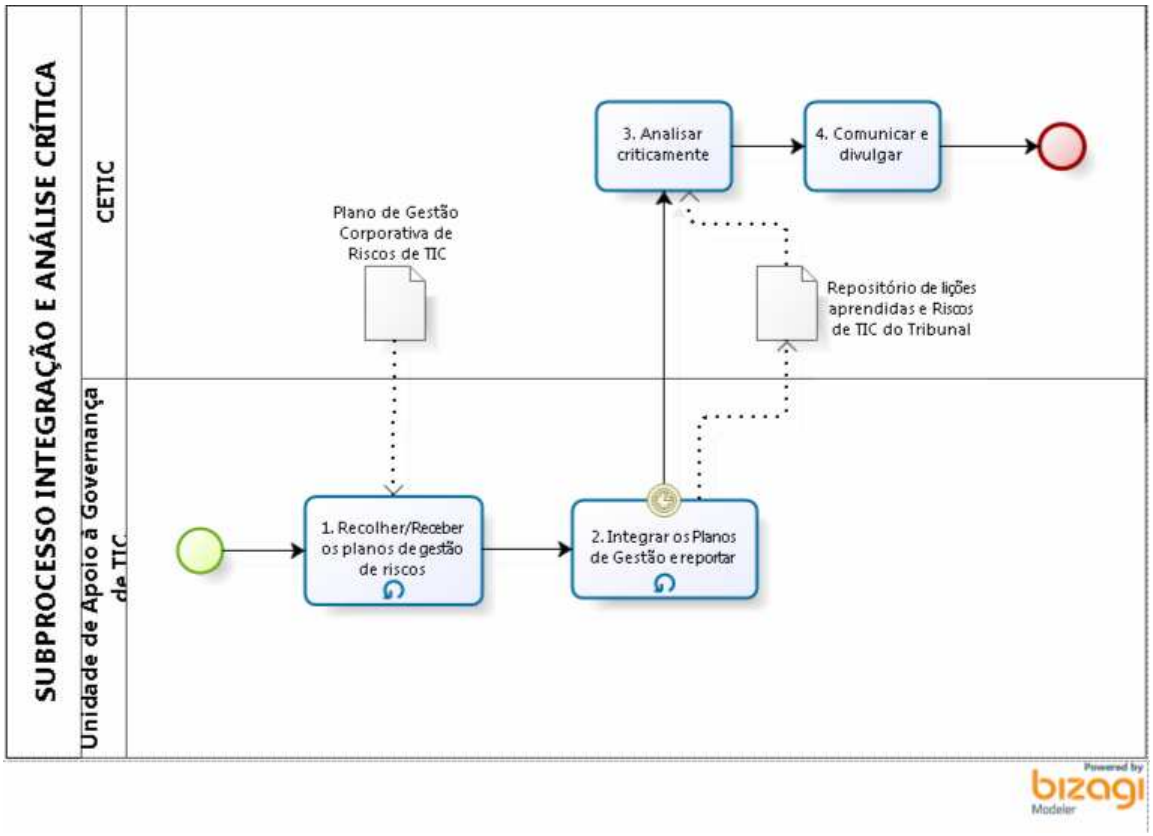
**Descrição**

Enviar Plano de Gestão Corporativa de Riscos de TIC atualizado à unidade de apoio à Governança de TIC, para integração, monitoramento e reporte ao CETIC, conforme desenho do processo.

**Executante**

Proprietário de Risco

# 5 INTEGRAÇÃO E ANÁLISE CRÍTICA



# 5.1 SUBPROCESSO INTEGRAÇÃO E ANÁLISE CRÍTICA

## 5.1.1 ELEMENTOS DO PROCESSO

### 5.1.1.1 1. Recolher/Receber os planos de gestão de riscos

**Descrição**

Receber os Planos de Gestão Corporativa de Riscos de TIC atualizados encaminhados pelos Proprietários de Risco, para fins de reporte ao CETIC, sempre que necessário, conforme desenho do processo.

**Executante**

Unidade de apoio à Governança de TIC

### 5.1.1.2 2. Integrar os Planos de Gestão e reportar

**Descrição**

Integrar o Plano de Gestão Corporativa de Riscos de TIC aos demais existentes, bem como as Lições Aprendidas no caso concreto, e condensar o resultado em um Repositório de Lições Aprendidas e Riscos de TIC, com o intuito de reportá-lo ao CETIC, sempre que necessário, para fins de análise crítica e melhoria do processo.

**Executante**

Unidade de apoio à Governança de TIC

### 5.1.1.3 3. Analisar criticamente

**Descrição**

Analisar criticamente os Planos de Gestão Corporativa de Riscos de TIC integrados com as Lições Aprendidas encaminhados pela unidade de apoio à Governança de TIC, bem como eventuais relatórios de Auditoria de Gestão de Riscos de TIC realizada pela unidade de Controle Interno e Auditoria ou equivalente, para fins de reporte ao CDTIC, se for o caso.

**Executante**

CETIC

#### 5.1.1.4  4. Comunicar e divulgar

**Descrição**

Comunicar ao CDTIC quaisquer informações relevantes que possam implicar atualização no Processo de Gestão Corporativa de Riscos de TIC, na Política Corporativa de Gestão de Riscos de TIC e no Modelo do Plano de Gestão Corporativa de Riscos de TIC (Anexo).

Eventualmente, se entender necessário, promover treinamento para os servidores envolvidos no processo.

**Executante**

CETIC

# 6 RECURSOS

## 6.1 CDTIC (ENTIDADE)

**Descrição**

Comitê Diretivo de Tecnologia da Informação e Comunicação

## 6.2 CETIC (ENTIDADE)

**Descrição**

Comitê Executivo de Tecnologia da Informação e Comunicação

## 6.3 PROPRIETÁRIO DE RISCO (FUNÇÃO)

**Descrição**

Pessoa ou entidade com a responsabilidade e autoridade para gerenciar um risco

## 6.4 UNIDADE DE APOIO À GOVERNANÇA DE TIC (FUNÇÃO)

**Descrição**

Unidade da área de tecnologia da informação responsável pelo apoio à Governança de TIC