



Enap

# Fiscalização e Gestão de Contratos de TIC

Módulo

## 3 Gerenciamento de riscos das contratações de TIC



## **Fundação Escola Nacional de Administração Pública**

### **Presidente**

Diogo Godinho Ramos Costa

### **Diretor de Desenvolvimento Profissional**

Paulo Marques

### **Coordenador-Geral de Produção Web**

Carlos Eduardo dos Santos

### **Equipe responsável**

Henry Mross (Conteudista, 2020);

Eleidimar Odília (Cordenadora-Geral, 2020);

Marcio Lima e Lucas Mota (Representantes da SGD/ME, 2020);

Iara da Paixão Corrêa (Coordenadora, 2020).

Priscila Callegari Reis (Coordenadora, 2020)

Haruo Silva Takeda (Coordenação Web, 2020)

Maria Karoline Domingues (Revisão de texto, 2020)

Ludmila Bravim da Silva (Revisão de texto, 2020)

Rodrigo Mady da Silva (Implementação Articulate e Moodle, 2020)

Israel Silvino Batista Neto (Direção e produção gráfica, 2020)

Ana Carla Gualberto Cardoso (Diagramação, 2020)

**Desenvolvimento do curso realizado no âmbito do acordo de Cooperação Técnica FUB / CDT / Laboratório LatITUDE e Enap.**

**Fonte das imagens modificadas e utilizadas no curso: freepik**

**Curso produzido em Brasília, 2020.**

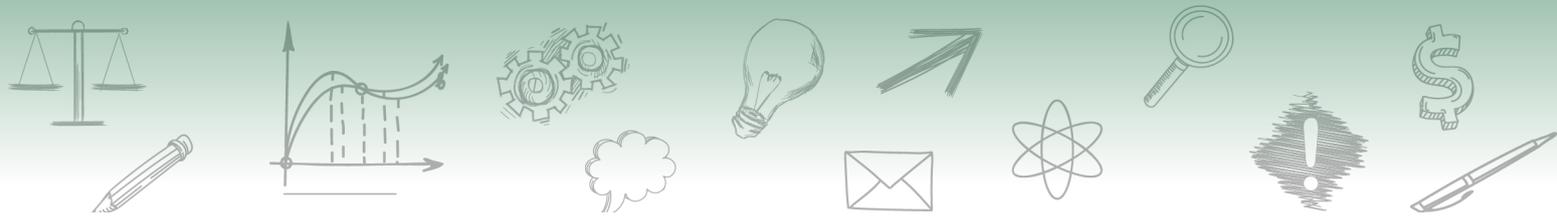


Enap, 2020

**Enap Escola Nacional de Administração Pública**

Diretoria de Educação Continuada

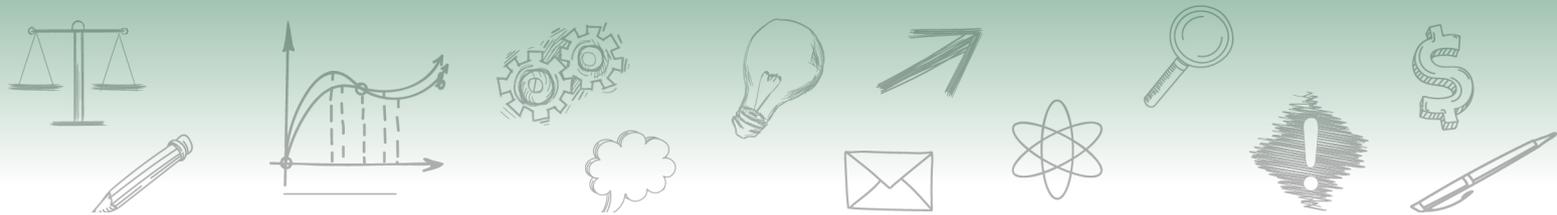
SAIS - Área 2-A - 70610-900 — Brasília, DF



# Sumário

<b>Unidade 1: Risco e Gerenciamento de Riscos .....</b>	<b>5</b>
1.1 Conceitos Iniciais .....	5
1.2 Relação custo x nível de risco.....	7
1.3 Riscos relacionados ao processo de contratação.....	10
1.4 Mapa de Gerenciamento de Riscos .....	13
<b>Unidade 2: Gerenciamento de Riscos na execução de contratos de TIC .....</b>	<b>16</b>
2.1. Gerenciamento de riscos na fase de Gestão Contratual....	16
2.2. Reduzindo riscos durante a execução .....	19
<b>Referências.....</b>	<b>23</b>





## Módulo

# 3 Gerenciamento de riscos das contratações de TIC

Neste módulo você aprenderá o conceito de risco e gerenciamento de risco; conhecerá o processo de gerenciamento de riscos para contratações de TIC; também aprenderá a construir o Mapa de Gerenciamento de Riscos (MGR) de contratações de TIC; E por fim, compreenderá a relação dos riscos mais comuns na fase de GCTIC e das práticas mais comuns para evitá-los.

O módulo está estruturado da seguinte maneira:

Unidade 1: Risco e Gerenciamento de Riscos

Unidade 2: Gerenciamento de Riscos na execução de contratos de TIC

## Unidade 1: Risco e Gerenciamento de Riscos

### 🎯 Objetivo de aprendizagem

**Ao final da unidade, você será capaz de reconhecer os conceitos básicos ligados à gestão de riscos em contratações de TIC.**

### 1.1 Conceitos Iniciais

Podemos começar este módulo admitindo que o risco é um fator inerente à atuação humana e de qualquer organização social. Qualquer passeio, viagem, compra, projeto, etc., e tudo o mais que fazemos está sempre sujeito a riscos.

Vamos nos situar sobre o que vem a ser o risco.

#### Conceito de risco

Há diversas definições na literatura, e podemos encontrar diferentes conceitos em normas técnicas, padrões e metodologias. Vejamos algumas:

- + Segundo a ABNT NBR ISO 31000 (norma técnica que trata de gestão de riscos)

Risco é o efeito da incerteza nos objetivos.



+ Segundo o PMBoK (conjunto de boas práticas para a gestão de projetos)

Risco é um evento ou condição incerta que, se ocorrer, terá um efeito positivo ou negativo sobre pelo menos um objetivo do projeto.

+ Segundo Antonio Celso Ribeiro Brasileiro, autor de um método de gestão e análise de riscos

Risco é uma condição que cria ou aumenta o potencial de perdas.

+ Segundo a IN MP/CGU nº 1/2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal

Risco é a possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade.

[IN MP/CGU nº 1/2016](#)

No que se refere a gerenciamento de riscos em contratações, estamos interessados nos **riscos que podem comprometer o sucesso da contratação**, em todas as fases.

Por isso o diagrama do MCTIC completo inclui o Gerenciamento de Riscos (GR), que não é exatamente uma fase, mas um processo contínuo que permeia todas as fases de uma contratação de TIC, desde o encaminhamento da demanda até o encerramento do contrato:

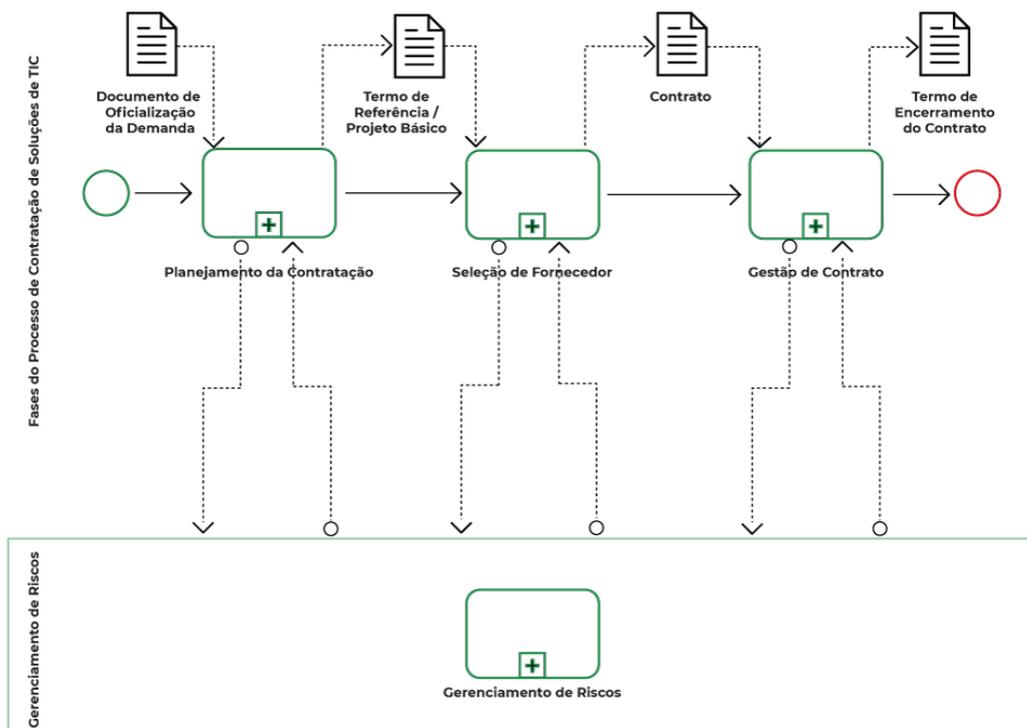
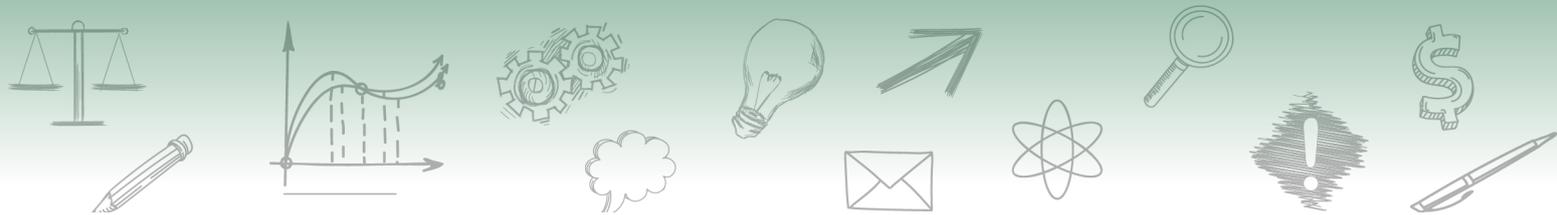


Figura 21 - MCTIC incluindo o processo de gerenciamento de riscos.



A IN SGD/ME nº 1/2019 apresenta, em suas definições, alguns conceitos iniciais relacionados ao gerenciamento de riscos que precisamos ter em conta:



*Art. 2º Para fins desta Instrução Normativa, considera-se:*

*XII - identificação de riscos: processo de busca, reconhecimento e descrição de riscos. Envolve a identificação das principais fontes de risco, eventos, suas causas e suas consequências potenciais. Também pode envolver dados históricos, análises teóricas, parecer de especialistas e as necessidades das partes interessadas;*

*XIII - nível de risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação dos impactos e de suas probabilidades;*

*XIV - tratamento de riscos: processo para responder ao risco, cujas opções, não mutuamente exclusivas, envolvem evitar, reduzir ou mitigar, transferir ou compartilhar, e aceitar ou tolerar o risco;*

*XV - análise de riscos: processo de compreensão da natureza do risco e determinação do nível de risco. Fornece a base para a avaliação de riscos e para as decisões sobre o tratamento de riscos;*

*XVI - avaliação de riscos: processo de comparar os resultados da análise de riscos para determinar se o risco e/ou sua magnitude é aceitável ou tolerável. A avaliação de riscos auxilia na decisão sobre o tratamento de riscos;*

*XVII - gerenciamento de riscos: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos da organização pertinentes com a contratação;*

*[...]*



Ao longo do nosso processo de gerenciamento de riscos, a depender da fase, a Equipe de Planejamento da Contratação ou a Equipe de Fiscalização do Contrato realiza as atividades definidas nesses incisos e avalia o nível de risco de forma empírica e subjetiva, mas buscando também um caráter objetivo nesta análise.

## 1.2 Relação custo x nível de risco

Vimos nas definições do tópico anterior que as ações de tratamento em geral envolvem alguns tipos de atividades, a saber:

### + Evitar riscos

Consiste em empregar ações que eliminam por completo o risco. Por exemplo, quando construímos um ETP, eliminamos o risco de termos responsabilidade por não planejar (ainda que possa restar algum risco de planejarmos mal). Por isso, devemos ser diligentes



quando realizamos nossos planejamentos, nos esforçando para pensar em todos os fatores e cenários possíveis.

#### + **Mitigar (ou reduzir) o riscos**

É quando utilizamos ações que atuam na diminuição da probabilidade de ocorrência ou da gravidade do impacto em caso de ocorrência do evento relacionado ao risco.

#### + **Transferir riscos**

Quando atribuímos o risco a terceiros. O exemplo clássico é a contratação de um seguro.

Quando utilizamos pagamento por entregas realizadas, métricas objetivas e aferição de qualidade em nossas contratações, na prática estamos transferindo o risco de baixa produtividade e de execução malfeita para a contratada.

#### + **Compartilhar riscos**

É integrar outros atores nas ações de tratamento de riscos. Por exemplo, a efetiva participação dos integrantes da Equipe de Planejamento da Contratação ou da Equipe de Fiscalização do Contrato é uma forma de compartilhar risco entre as áreas. A ampliação da equipe, incluindo demandantes de diversas áreas da instituição, também é um exemplo de compartilhamento de riscos.

As contratações conjuntas, desde que equipes de diversas instituições participem do planejamento, consistem em mecanismo de redução de custos, mas, em um certo sentido, também de compartilhamento de riscos.

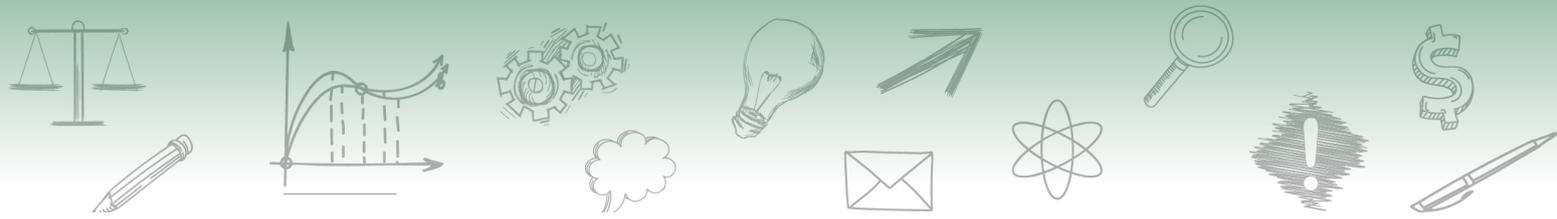
#### + **Aceitar ou tolerar riscos**

Consiste em decidir por não realizar ações prévias de tratamento, sujeitando-se à ocorrência do evento relacionado ao risco (que se desejaria evitar), diante da baixa probabilidade ou impacto que poderia causar, ou ainda de seu alto custo.

Por exemplo: tolera-se o risco de indisponibilidade temporária de um painel de análise dos dados, considerando que tal atividade não possui alta criticidade para a instituição, em comparação com a disponibilidade de um sistema portuário de aduana, posto que sua paralisação poderia causar prejuízos consideráveis para diversos atores envolvidos.

Essas ações têm muito a ver com o conceito de **apetite a risco**, que pode ser definido como o grau de exposição a que pessoas e organizações estão dispostas a correr riscos. Isto é, a disposição em aceitar o risco sem realizar ações preventivas de efetiva redução de probabilidade ou impacto, ou realizando ações de pouca ou menor efetividade.

Caso optemos por aceitar determinado risco - ou mesmo se não tivermos alternativa, a não ser correr o risco - devemos definir ações de contingência para o caso de ocorrer o evento associado a ele, isto é, o evento que queremos evitar.



## SAIBA MAIS

### O que é uma ação de contingência?

Podemos dizer que uma ação de contingência é um tipo de tratamento que consiste em lançar mão de novos recursos, procedimentos ou mecanismos, em substituição aos recursos atingidos ou prejudicados por eventos indesejados, para atingir total ou parcialmente o resultado originalmente esperado.

Exemplos de ações de contingência:

- baixar um backup em caso de pane de sistemas e perda de dados;
- utilizar um notebook quando o desktop falhar.

Um contraexemplo com o qual muitos colegas se atrapalham: aplicar uma penalidade NÃO é uma ação de contingência, pois não substitui o cumprimento da obrigação por parte da contratada!

(Mas, sim, pode ser encarada como ação de mitigação do risco de futuras novas ocorrências..).

Evidentemente, a questão do custo do tratamento de riscos tem alta relevância na definição das ações preventivas de extinção, mitigação, transferência dos riscos, bem como nas possíveis ações de contingência.

Numa suposição livre, poderíamos considerar que - em muitos casos - a relação entre custo e prevenção de riscos em geral tem um comportamento assemelhado ao do gráfico a seguir:



Figura 22 - Relação entre custos da prevenção e exposição a riscos.

Assim, a grande questão quando se tem limitações de recursos seria buscar o centro do gráfico, encontrando ações de baixo custo, mas que possuam grande efetividade na prevenção.



A parte vermelha da curva expressa possivelmente um descuido ou apetite exagerado ao risco, enquanto a parte azul, um viés de controle exagerado, o qual pode custar mais caro que o próprio objeto que estamos buscando proteger.

## DESTAQUE

Por exemplo: após um evento de furto de um notebook (que era utilizado por um programador) em suas dependências, e cujo valor era de aproximadamente R\$ 7 mil, uma certa diretoria de determinada instituição solicitou a instalação de um sistema de sensor de RFID para prevenir novos incidentes do tipo. O valor orçado do sistema só para os notebooks montou em cerca de R\$ 4 milhões. Verificou-se que havia 12 anos que não se registravam furtos na sede da instituição.

Você autorizaria essa contratação? Pensaria em outras alternativas? Que tal chamar uma seguradora?

### 1.3 Riscos relacionados ao processo de contratação

O processo definido de gerenciamento de riscos da IN SGD/ME nº 1/2019 prevê a execução das atividades de tratamento e atualização dos controles de riscos ao longo de todo o ciclo da contratação, como vemos no diagrama a seguir:

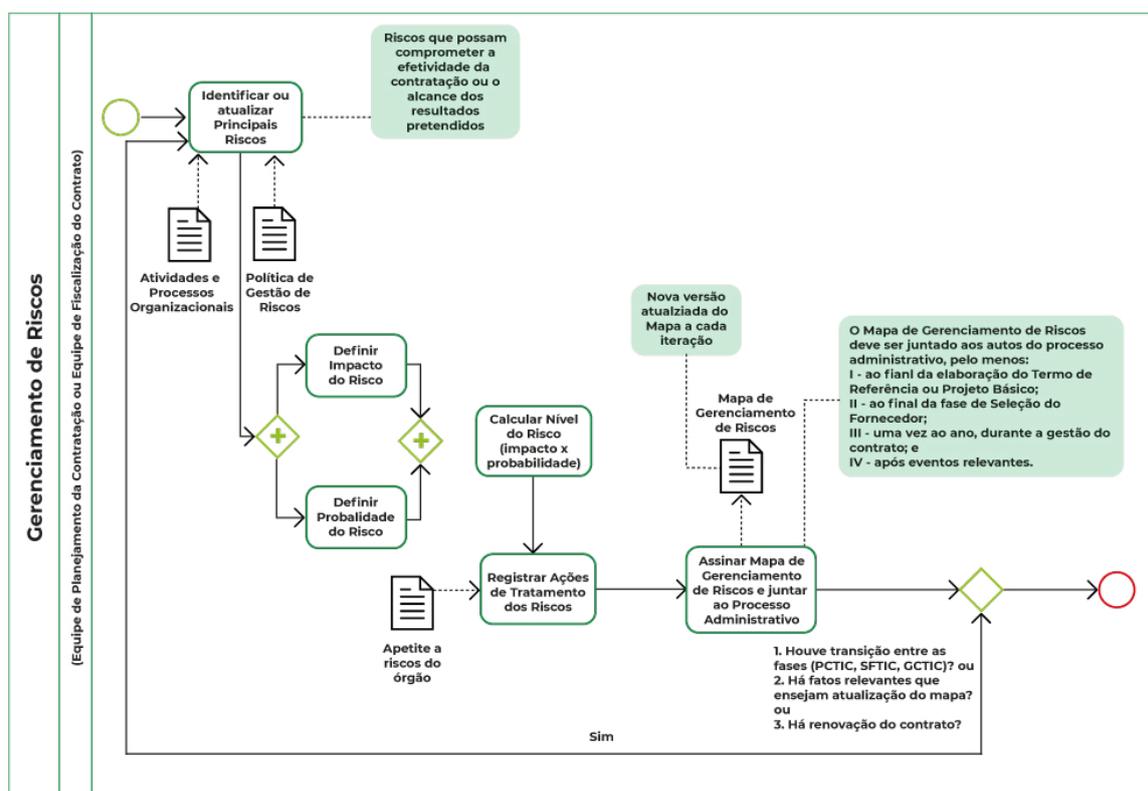
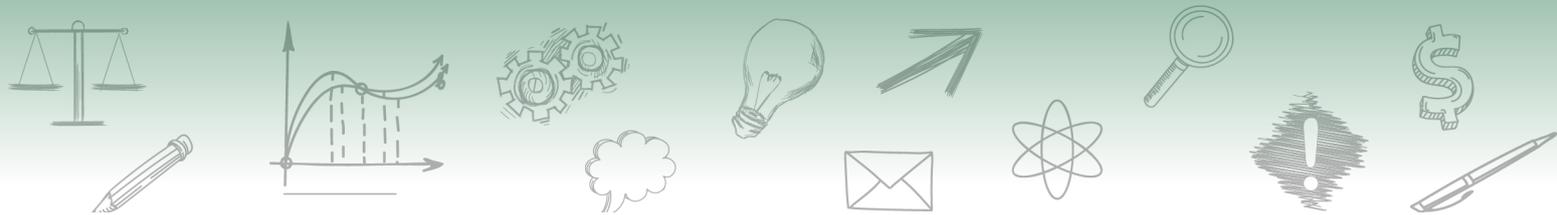


Figura 23 - O processo definido de gerenciamento de riscos da IN SGD/ME nº 1/2019.



Esse processo está completamente descrito no artigo 38 da IN SGD/ME nº 1/2019. Vejamos, por enquanto, somente a definição dos responsáveis por realizar e liderar as execuções dessas tarefas:



*Art. 38. O gerenciamento de riscos deve ser realizado em harmonia com a Política de Gestão de Riscos do órgão prevista na Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016.*

*§ 1º Durante a fase de planejamento, a equipe de Planejamento da Contratação deve proceder às ações de gerenciamento de riscos e produzir o Mapa de Gerenciamento de Riscos que deverá conter no mínimo:*

*I - identificação e análise dos principais riscos, consistindo na compreensão da natureza e determinação do nível de risco, mediante a combinação do impacto e de suas probabilidades, que possam comprometer a efetividade da contratação, bem como o alcance dos resultados pretendidos com a solução de TIC;*

*II - avaliação e seleção da resposta aos riscos em função do apetite a riscos do órgão; e*

*III - registro e acompanhamento das ações de tratamento dos riscos.*

*§ 2º Durante a fase de Seleção do Fornecedor, o Integrante Administrativo com apoio dos Integrantes Técnico e Requisitante deve proceder às ações de gerenciamento dos riscos e atualizar o Mapa de Gerenciamento de Riscos.*

*§ 3º Durante a fase de Gestão do Contrato, a Equipe de Fiscalização do Contrato, sob coordenação do Gestor do Contrato, deverá proceder à atualização contínua do Mapa de Gerenciamento de Riscos, realizando as seguintes atividades:*

*I - reavaliação dos riscos identificados nas fases anteriores e atualização de suas respectivas ações de tratamento; e*

*II - identificação, análise, avaliação e tratamento de novos riscos.*

*[...]*



Essa sequência está baseada no processo de gestão de riscos definido na ISO 31000:2018, representado na figura a seguir:



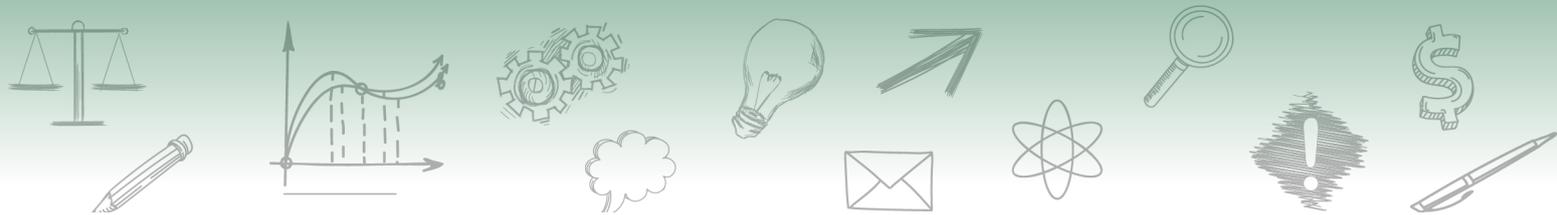
Figura 24 - O processo da ISO 31000:2018.

O escopo e o contexto neste caso estão basicamente definidos, considerando que estamos tratando especificamente do processo de contratação de uma determinada solução de TIC.

Assim, ao contratarmos, por exemplo, uma solução de banco de dados, não vamos tratar do risco de perda de informações por falta de energia, pois esse é um risco corporativo do ambiente computacional e está fora do escopo da contratação. Mas obviamente é boa prática nos assegurarmos de que isso está sendo devidamente tratado na área de infraestrutura de TIC da organização.

## DESTAQUE

O critério será uma classificação quali-quantitativa de criticidade. Para o registro utilizaremos o MGR. O relato será feito no próprio MGR, nos artefatos produzidos ao longo da contratação e no processo administrativo.



## 1.4 Mapa de Gerenciamento de Riscos

O Mapa de Gerenciamento de Riscos (MGR) é o artefato que consolida as análises de riscos realizadas durante o processo de contratação. Ele está definido no "arcabouço das definições" da IN SGD/ME nº 1/2019:



*Art. 2º Para fins desta Instrução Normativa, considera-se:*

*[...]*

*XVIII - Mapa de Gerenciamento de Riscos: instrumento de registro e comunicação da atividade de gerenciamento de riscos ao longo de todas as fases da contratação;*



Portanto, o MGR é um documento vivo, atualizado ao longo de todo o processo definido do Modelo de Contratação de Soluções de TIC (MCTIC).

A IN SGD/ME nº 1/2019 definiu a periodicidade mínima com que o MGR deve ser atualizado:



*Artigo 38:*

*§ 4º O Mapa de Gerenciamento de Riscos deve ser juntado aos autos do processo administrativo, pelo menos:*

*I - ao final da elaboração do Termo de Referência ou Projeto Básico;*

*II - ao final da fase de Seleção do Fornecedor;*

*III - uma vez ao ano, durante a gestão do contrato; e*

*IV - após eventos relevantes.*



Para construção do MGR, podemos utilizar um formulário ou um aplicativo de planilha eletrônica.

Para realizar as atividades de identificação de riscos, avaliação de probabilidade de ocorrência, impacto do evento associado a cada risco e posterior registro das respectivas ações de tratamento, utilizam-se técnicas conhecidas na literatura e no mercado. Algumas dessas técnicas são apresentadas na figura a seguir:



Atividade	Ferramenta
Identificação de riscos	<ul style="list-style-type: none"> <li>- Brainstorming</li> <li>- Histórico de contratações anteriores</li> <li>- Paradigmas</li> <li>- Análise de cenários</li> <li>- Checklist</li> </ul>
Análise de riscos	<ul style="list-style-type: none"> <li>- Matriz de vulnerabilidade (probabilidade x impacto)</li> </ul>
Avaliação de riscos	<ul style="list-style-type: none"> <li>- Matriz de priorização</li> </ul>
Ações de tratamento	<ul style="list-style-type: none"> <li>- Diagrama de causa e efeito (Ishikawa)</li> <li>- Análise swot</li> <li>- 5W2H</li> </ul>

Figura 25 - Técnicas e ferramentas para atividades de gerenciamento de riscos.

A seguir, você verá as breves explicações sobre as ferramentas:

**+ Brainstorming**

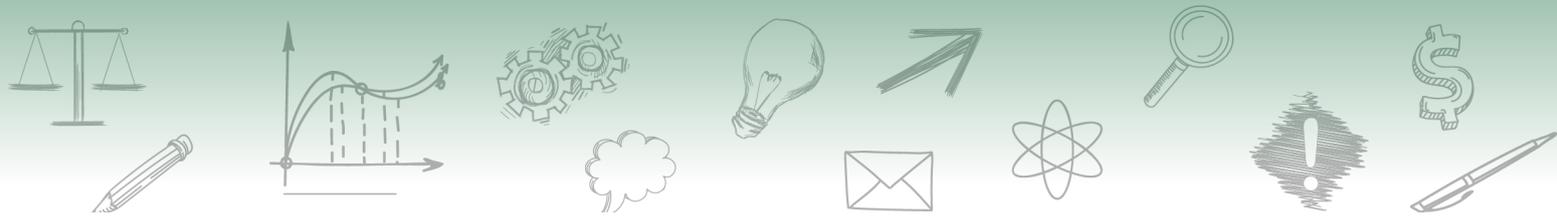
Também conhecido como "tempestade de ideias", pode ser traduzido do inglês como "debate". Mas, mais que um debate, consiste em uma verdadeira dinâmica de grupo em que os participantes devem se sentir livres para apresentar e discutir ideias, cenários, possibilidades de desdobramento de causas e efeitos e possíveis soluções, explorando sua criatividade.

Para saber mais, consulte <https://pt.wikipedia.org/wiki/Brainstorming>

**+ Análise SWOT**

Também conhecido em português por Análise FOFA (Forças, Oportunidades, Fraquezas e Ameaças), consiste originalmente em uma técnica de diagnóstico institucional criada para elaboração de planejamentos estratégicos. Mas pode ser aplicada para qualquer tipo de análise de contexto. Na análise de riscos de contratações, auxilia na identificação e mensuração da criticidade dos riscos associados ao processo e ao objeto da contratação, bem como na definição de ações de tratamento.

Para saber mais, consulte [https://pt.wikipedia.org/wiki/An%C3%A1lise\\_SWOT](https://pt.wikipedia.org/wiki/An%C3%A1lise_SWOT)



#### + **Diagrama de Ishikawa**

Também conhecido por Diagrama de Causa e Efeito ou de Espinha de Peixe, foi proposto originalmente para analisar a relação entre um efeito e suas possíveis causas. Pode ser utilizado para investigar as causas dos riscos e definir ações de tratamento.

Para saber mais, consulte [https://pt.wikipedia.org/wiki/Diagrama\\_de\\_Ishikawa](https://pt.wikipedia.org/wiki/Diagrama_de_Ishikawa)

#### + **5W2H**

Acrônimo em inglês que significa as principais perguntas feitas para se analisar um fato, contexto ou processo: What (o que?), Why (por que?), Who (quem?), When (quando?), Where (onde?), How (como?), How much (quanto?). No gerenciamento de riscos, permite aprofundar as características e condições das ações de tratamento.

Para saber mais, consulte <https://pt.wikipedia.org/wiki/5WH>

#### + **Checklist**

Em análises de riscos, Listas de Verificação são utilizadas para identificar riscos, efeitos ou boas práticas comumente observados em contratações anteriores ou inerentes a qualquer contratação. Uma lista previamente preparada pode ser confrontada com a contratação ou objeto em pauta. Podem ser utilizadas individualmente ou em reuniões ou sessões de tempestade de ideias, ou ainda associadas a outras ferramentas, como as acima.

Para saber mais, consulte [https://pt.wikipedia.org/wiki/Lista\\_de\\_verifica%C3%A7%C3%A3o](https://pt.wikipedia.org/wiki/Lista_de_verifica%C3%A7%C3%A3o)

#### + **Matrizes de Priorização, Risco, Vulnerabilidade e/ou Criticidade**

São matrizes utilizadas para selecionar os principais riscos a serem tratados, em razão da probabilidade de ocorrência do evento associado e do seu consequente impacto para o processo ou negócio. Veremos um exemplo na próxima unidade.



## Unidade 2: Gerenciamento de Riscos na execução de contratos de TIC

### 🎯 Objetivo de aprendizagem

Ao final desta unidade, você será capaz de reconhecer o passo-a-passo para a construção do artefato Mapa de Gerenciamento de Riscos (MGR) na fase de GCTIC; e conhecer algumas dicas importantes e alguns riscos comuns desta fase.

### 2.1. Gerenciamento de riscos na fase de Gestão Contratual

Os principais riscos associados ao processo definido de contratação de soluções de TIC são classificados em dois grupos:

#### + Riscos de processo

São aqueles que podem comprometer o sucesso do processo de contratação em qualquer das suas fases. Estão associados à eficiência, eficácia e economicidade da contratação.

#### + Riscos de produto

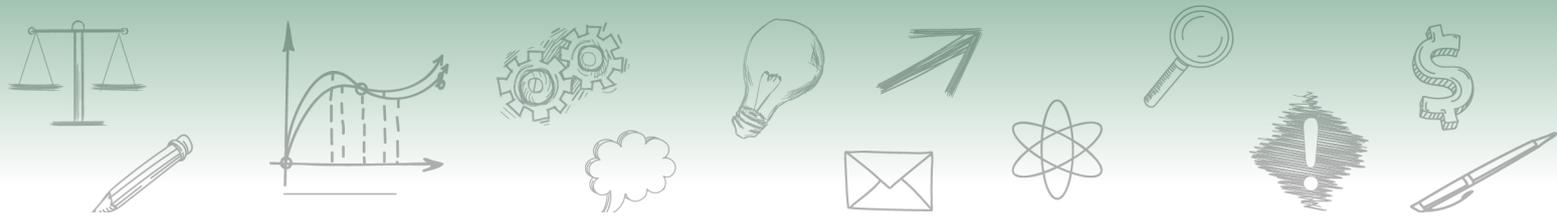
São os de que a solução de TIC não atenda às necessidades para cujo atendimento foi contratada. Estão associados à efetividade da contratação.

O Gerenciamento de Riscos – GR é um processo contínuo que permeia todas as fases do MCTI e - conforme o parágrafo 4º do artigo 38 da IN SGD/ME nº 1/2019 -, ao iniciar-se o GCTIC, já teremos pelos menos duas versões do MGR no processo administrativo, relativas às duas fases anteriores da contratação, isto é, ao Planejamento da Contratação de TIC (PCTIC) e à Seleção do Fornecedor de TIC (SFTIC).

Assim sendo, ao iniciar-se o GCTIC, a primeira coisa recomendável para a EFC fazer, no que tange ao Gerenciamento de Riscos, seria analisar os MGRs anteriores, para implementar as medidas de tratamento que tenham sido propostas para a fase do GCTIC.

Devemos também reavaliar estes riscos e, se for o caso, propor e implementar novas medidas em reforço ou substituição àquelas.

Nesse sentido, estaremos realizando o disposto no inciso I do parágrafo 3º do artigo 38 da IN SGD/ME nº 1/2019:



Art. 38

[...]

§ 3º Durante a fase de Gestão do Contrato, a Equipe de Fiscalização do Contrato, sob coordenação do Gestor do Contrato, deverá proceder à atualização contínua do Mapa de Gerenciamento de Riscos, realizando as seguintes atividades:

**I - reavaliação dos riscos identificados nas fases anteriores e atualização de suas respectivas ações de tratamento; e**

**II - identificação, análise, avaliação e tratamento de novos riscos.**

[...](grifo nosso).



Em geral, as ações que vamos implementar neste momento correspondem a riscos de produto identificados, analisados e avaliados principalmente na fase de PCTIC. Portanto, são ações que buscam garantir a efetividade do objeto em face das necessidades de negócio.

Entretanto, não quer dizer que não haja riscos de processo nesta fase, destacando-se entre eles os riscos relacionados ao processo de fiscalização do contrato.

Em vista disso, e em que pese o fato de o mesmo parágrafo 4º do artigo 38 estabelecer tão-somente que, durante o GCTIC, é obrigatório produzir uma nova versão deste artefato pelo menos uma vez ao ano, não seria mal considerar que:

## DESTAQUE

É recomendável que a EFC construa o primeiro MGR do GCTIC logo ao início do contrato.

Naturalmente, os conhecimentos relativos à execução, fiscalização e gestão do contrato nem sempre são de rápido aprendizado. E não é raro que a prática do dia-a-dia da gestão e fiscalização ajude a EFC a descobrir pontos fracos e novos riscos.

Nesse sentido, a EFC deve avaliar o melhor momento para produzir sua primeira versão do MGR. Feito isso, o processo de GR permanece em execução até o final do contrato, construindo-se tantas novas versões deste artefato quantas forem necessárias, considerando o disposto no §4º do art. 38:



Art. 38

[...]

§ 4º O Mapa de Gerenciamento de Riscos deve ser juntado aos autos do processo administrativo, pelo menos:



[...]

III - uma vez ao ano, durante a gestão do contrato; e

IV - após eventos relevantes.

[...] (grifo nosso).

Por conseguinte, a construção de novas versões do MGR deve incluir sempre:

- a. A reavaliação dos riscos que integram as versões anteriores do MGR.
- b. A identificação, análise, avaliação e tratamento de novos riscos, sejam eles de processo ou de produto.

Para essas atualizações, pode-se usar, por exemplo, uma matriz de criticidade com classificação de probabilidade e impacto como a da figura a seguir:

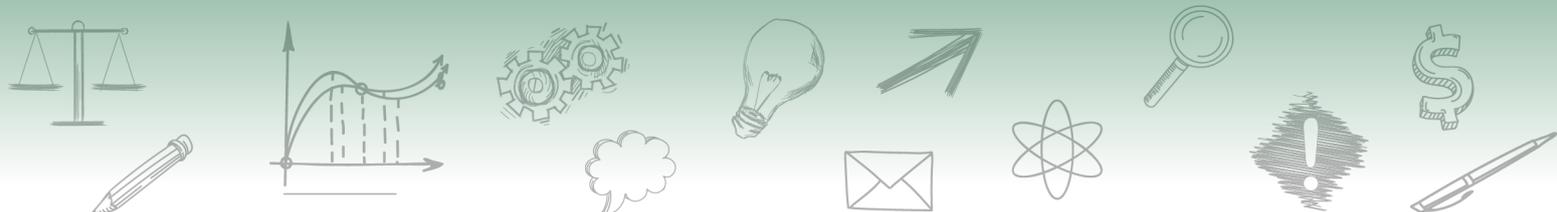
Impacto Probabilidade	Baixo	Médio	Alto
Alta			R1
Média	R4	R12	R8, R9
Baixa		R5, R6, R7	R2, R3, R10, R11

Figura 26- Matriz de criticidade (o “R” seguido de ordinais representa um erro identificado)

Para os riscos mais críticos, deve-se necessariamente programar o tratamento adequado, considerando o contexto da execução do contrato.

Os riscos considerados menos críticos podem ou não ser tratados, de acordo com o consumo de recursos - não somente financeiros, como também em termos do tempo, pessoas, esforço ou outros - que as ações demandem.

Todas essas atividades são registradas, portanto, em uma nova versão do MGR.



Ao mesmo tempo, devemos acompanhar a aplicação das ações de tratamento que já haviam sido definidas e registrar tudo no MGR. Este processo contínuo está representado no diagrama a seguir.

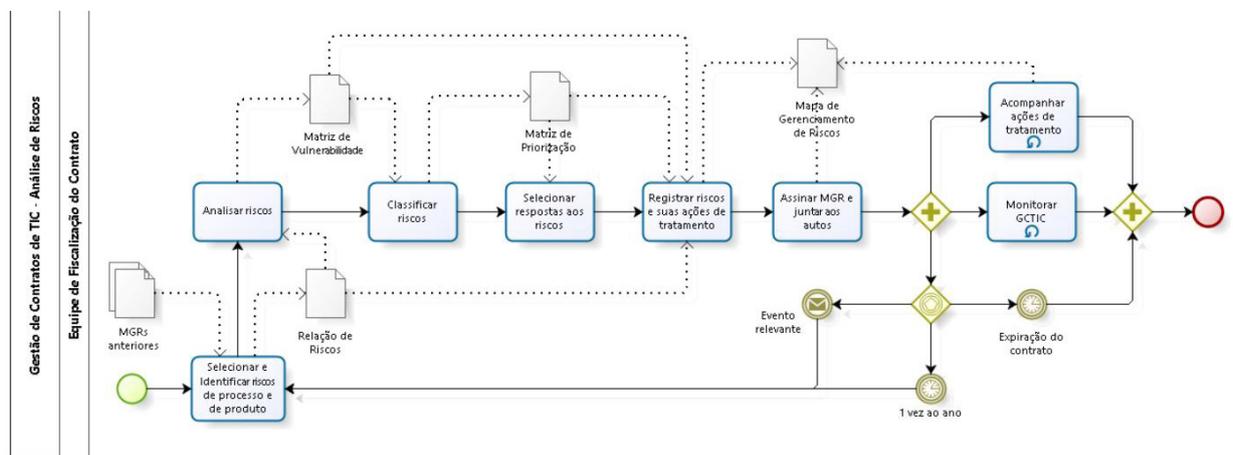


Figura 27 - Processo detalhado de gerenciamento de riscos durante a fase de GCTIC

O [template do Mapa de Gerenciamento de Riscos](#) da SGD/ME materializa na prática este processo de realização das atividades de gerenciamento de riscos.

Vale destacar que muitas vezes tomamos decisões ao longo do GCTIC baseados em novos riscos identificados, mas não registrados. Parece que intuímos o risco, mas não o racionalizamos em forma de reflexão.

Por exemplo: Se, na qualidade de fiscais, percebemos que alguns colegas estão utilizando a tampa de impressoras locadas para colocar seu copo de cafezinho e afixamos um aviso em todas as impressoras para evitar esta prática, estamos mitigando o risco de defeito causado pelo mau uso de equipamento, sujeito a apuração de responsabilidade e ressarcimento à contratada. Mas nem sempre documentamos isso no nosso GCTIC!

Neste caso, esta condição deve ser descrita tanto no MGR quanto no histórico do contrato e, caso não tenha sido identificado anteriormente, o risco deve ser incorporado ao MGR. Então:

## DESTAQUE

Devemos assimilar a boa prática de registrar a identificação e o acompanhamento do tratamento de riscos no MGR, documentando inclusive como este tratamento se refletiu ao longo da execução do contrato.

## 2.2. Reduzindo riscos durante a execução

O texto a seguir relaciona alguns dos riscos mais comuns da fase de GCTIC, para os quais a EFC deve sempre atentar, definindo e implementando as devidas ações de tratamento:



**+ Risco de falhas na gestão e fiscalização do contrato.**

Logicamente, quanto maior a complexidade do objeto contratado, mais complicada será a gestão e fiscalização do contrato. Mas de toda forma, o risco de ocorrerem deficiências na fiscalização - principalmente quando envolve verificações técnicas - está sempre presente.

Mas existem muitas medidas das quais podemos lançar mão para mitigar este risco, e elas devem ser oportuna e apropriadamente implementadas pela EFC, e de acordo com a necessidade. Tais como:

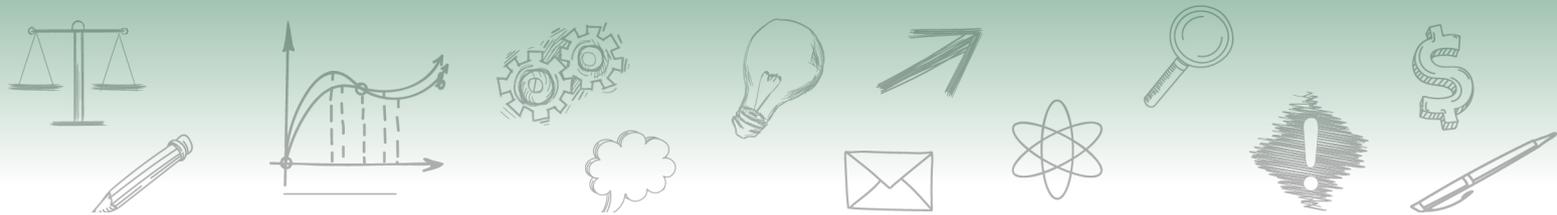
- realizar a revisão de análises de relatórios ou medições por pares, que podem ser servidores da área técnica ou requisitante envolvida, ou ainda fiscais substitutos;
- reforçar a EFC, designando mais atores para atuar no papel de fiscal, cada qual responsável sobre determinadas etapas ou conjuntos de elementos da fiscalização;
- utilizar ferramentas automatizadas e/ou planilhas para assegurar a precisão de cálculos;
- contratar empresas para prestar serviços de apoio às fiscalizações;
- implantar produtos de software de monitoramento para assegurar a precisão das medições;
- realizar processo formal de passagem de conhecimento e atualização para fiscais substitutos para que estejam preparados em casos de ausência - programada ou não - dos titulares;
- utilizar amplamente agendas e outras ferramentas de alertas eletrônicos para evitar perda de prazos contratuais; por exemplo: OSs mensais devem ser entregues ao preposto antes do início da prestação dos serviços relacionados, pagamentos devem ser realizados dentro do prazo estipulado no contrato, encaminhamento de solicitações de renovação do contrato devem atender ao disposto no artigo 36 da IN SGD/ME nº 1/2019, etc.

**+ Risco de haver falta de compromisso das áreas clientes envolvidas na execução, implantação ou utilização da solução.**

Nos casos de contratações de produtos ou de serviços de desenvolvimento de soluções de TIC, pode ocorrer desinteresse ou indisponibilidade por parte dos supostos beneficiários das áreas requisitantes, o que em geral acarreta atrasos ou mesmo desperdício de recursos.

Nessas situações pode-se tomar algumas atitudes preventivas:

- solicitar indicação formal de servidores da área requisitante pela autoridade competente para participar do projeto, responsabilizando-se pelos recebimentos, e podendo inclusive compor a EFC na qualidade de Fiscais Requisitantes - posto que, como já vimos, cada papel pode ser desempenhado por vários atores, cada qual com suas responsabilidades específicas;
- solicitar a publicação de normativo estabelecendo a obrigatoriedade das áreas



requisitantes de utilizar a solução de TIC como ferramenta de trabalho;

- realizar publicações ou eventos internos para comunicar o projeto e os benefícios e potencialidades da solução ao seu público-alvo.

#### + **Risco de inefetividade da solução.**

Este é o típico risco de produto, quase sempre presente na execução contratual. Principalmente em contratos de serviços, pode ocorrer que a solução não atenda adequadamente às necessidades de negócio ao longo da execução, gerando insatisfação nos usuários, bem como a degradação da imagem do contrato, da contratada, da área de TIC ou mesmo da instituição como um todo.

Portanto, deve-se acompanhar com cuidado os indicadores de resultados relacionados à efetividade da solução, o que em geral também inclui a percepção dos clientes dos serviços quanto à sua qualidade.

Para mitigar este risco ou tratar os efeitos enquanto os problemas ainda forem sanáveis, podemos:

- realizar a avaliação de qualidade e verificação dos critérios de aceitação das entregas com o rigor necessário, para evitar que inconformidades interfiram nos resultados esperados;
- realizar pesquisas de satisfação com os usuários e criar mecanismos de ouvidoria;
- realizar reuniões de ponto de controle com os principais interessados, visando avaliar resultados e identificar possíveis falhas ou fragilidades;
- realizar alterações contratuais para ajustar procedimentos, mecanismos de controle, condições operacionais e/ou volumes contratados, tendo em conta os limites da legislação pertinente, bem como a disponibilidade orçamentária.

#### + **Risco de demandar tarefas não previstas em contratos de serviços.**

É um dos riscos mais comuns em contratos de serviços de TIC e particularmente grave, pois afronta a vedação do art. 5º, IV da IN SGD/ME nº 1/2019

Nesse sentido, não é raro observarmos profissionais de empresas contratadas para prestar exclusivamente serviços de TIC realizando indevidamente tarefas como transporte de equipamentos e apoio administrativo, por exemplo.

Algumas medidas que podem ser tomadas para coibir esta irregularidade são:

- comunicar com precisão os serviços disponíveis no contrato para todos os possíveis usuários; por exemplo:
  - encaminhar e-mails preventivos de esclarecimento na lista corporativa;
  - em um contrato de service desk, divulgar o catálogo de serviços na intranet (aliás, esta é uma recomendação do [Guia de Service Desk da SGD/ME](#));



- utilizar uma ferramenta automatizada ou um processo específico de abertura e filtragem das demandas por pessoal autorizado.

+ **Risco de indicação indevida de profissionais para trabalhar na contratada em contratos de serviços.**

Também é caso de irregularidade, conforme o disposto no art. 5º, III e pode caracterizar crime de advocacia administrativa, nos termos do art. 123 do Código Penal ([Decreto-Lei nº 2.848/1940](#)).

Algumas ações de tratamento que podemos utilizar para evitar este risco são:

- alertar os representantes da contratada antes de iniciar a execução (ou no máximo até a reunião inicial) quanto a esta vedação, alertando, porém, que a mera contratação de profissionais que já prestaram serviços para o contratante não é vedada, desde que resultantes de iniciativa da própria contratada;
- recomendar à comissão de ética da instituição para realizar ampla divulgação aos servidores sobre esta vedação;
- ao identificar que esta prática foi efetivada, solicitar à contratada a substituição do profissional e tomar as demais medidas cabíveis.

+ **Risco de estabelecer relações informais de subordinação com profissionais da contratada.**

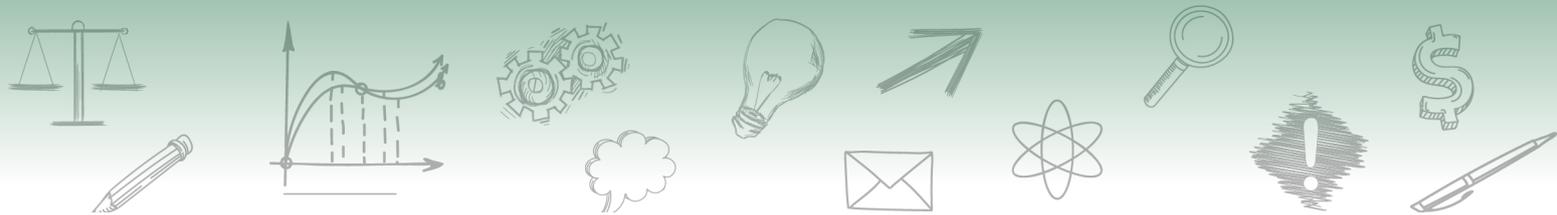
Também é um risco frequente de violação de vedação da IN SGD/ME nº 1/2019 (artigo. 5º, I), principalmente em casos de proximidade no dia-a-dia da execução contratual. Este risco é particularmente elevado em contratos de serviços por postos de trabalho - modelo que não é recomendado pela IN SGD/ME nº 1/2019 (vide inciso IX do mesmo artigo 5º). As ações de mitigação são semelhantes às apresentadas nos riscos anteriores:

- utilizar uma ferramenta automatizada ou um processo específico e formal de encaminhamento de demandas de tarefas específicas;
- realizar ampla divulgação desta vedação aos usuários dos serviços por meio de ferramentas institucionais (boletins, comunicados em listas de e-mail corporativas, apoio da comissão de ética, etc.);
- ao identificar que esta prática foi efetivada, comunicar formalmente o servidor e tomar as demais medidas cabíveis.

## DESTAQUE

Jamais se deve negligenciar o processo de Gerenciamento de Riscos durante a execução do contrato.

O gerenciamento de riscos está presente em todos os frameworks, metodologias e boas práticas que apoiam a TIC e o próprio negócio das instituições, portanto é um processo muito importante.



Às vezes as equipes encaram este processo como mera formalidade e não realizam as ações em toda a sua completude, e da forma cuidadosa e diligente como deve ser.

Mas podemos dizer sem exagero que:

## DESTAQUE

Executar um processo caprichado de gerenciamento de riscos eleva a segurança da execução e a qualidade das entregas do contrato.

Espero que nossos estudos tenham sido úteis para você e sirvam como um bom princípio para quem está iniciando no assunto ou um bom instrumento para aprimorar as práticas de gestão e fiscalização de contratos de TIC para aqueles que já as conheciam.

Boa sorte a todos nós na gestão, fiscalização e execução de contratos de TIC!

## Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 31000:2018**: Gestão de riscos - Diretrizes. Rio de Janeiro, 2018.

BRASÍLIA. Ministério da Economia. Secretaria Especial de Desburocratização, Gestão e Governo Digital. Secretaria de Governo Digital. **Instrução Normativa nº 1, de 4 de abril de 2019**. Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal. Diário Oficial da União. Brasília, 05 de abril de 2019. Disponível em: [https://www.in.gov.br/materia/-/asset\\_publisher/Kujrw0TZC2Mb/content/id/70267659/do1-2019-04-05-instrucao-normativa-n-1-de-4-de-abril-de-2019-70267535](https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/70267659/do1-2019-04-05-instrucao-normativa-n-1-de-4-de-abril-de-2019-70267535). Acesso em 19 out.2020.

BRASILIANO, Antônio Celso Ribeiro. **Resposta aos riscos corporativos – método brasileiro**. São Paulo: Sicurezza, 2009.

PROJECT MANAGEMENT INSTITUTE. **Um guia do Conjunto de Conhecimentos do Gerenciamento de Projetos - PMBoK**. 5 ed. Newtown Square: PMI Publications, 2013.