



Ministério da Educação  
Secretaria de Educação Profissional e Tecnológica  
Instituto Federal de Educação, Ciência e Tecnologia do Tocantins  
Reitoria

## PLANO DE GESTÃO DE RISCOS EM TECNOLOGIA DA INFORMAÇÃO

Este documento dispõe sobre o Plano de Gestão de Riscos em Tecnologia da Informação no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Estado do Tocantins (IFTO).

### 1. INTRODUÇÃO

A sistematização da gestão de riscos em nível institucional constitui estratégia que aumenta a capacidade da organização para lidar com incertezas, estimula a transparência, contribui para o uso eficiente de recursos públicos e melhora a entrega de serviços ao cidadão (TCU, 2018). Para HMG (2020), as organizações do setor público não podem ser avessas ao risco e ter sucesso, pois o risco é inerente a tudo o que fazemos para oferecer serviços de alta qualidade.

Neste contexto, este documento visa orientar as atividades a serem conduzidas de forma coletiva em reuniões de planejamento da área de Tecnologia da Informação (TI), de forma a prever eventos ou situações que possam comprometer a execução dos objetivos estratégicos definidos no Plano Diretor de TI (2020-2024). Com isso, espera-se aumentar a probabilidade e o impacto dos eventos positivos, reduzir a probabilidade e o impacto dos eventos negativos, e orientar a equipe de TI sobre como os riscos deverão ser gerenciados.

Sendo assim, o Plano de Gestão de Riscos de Tecnologia da Informação do IFTO contribui para a identificação de possíveis ameaças que poderão afetar o dia a dia organizacional, possibilitando agir proativamente, o que reduzirá os impactos negativos na missão e nos objetivos estratégicos de TI.

#### 1.1. Objetivo

O Plano de Gestão de Riscos em Tecnologia da Informação tem o objetivo de ser parte integrante da tomada de decisão informada desde o início da política ou do projeto, passando pela implementação até a entrega diária de serviços de Tecnologia da Informação. Este documento fornece uma abordagem para a gestão de riscos relacionados à Tecnologia da Informação por meio de um conjunto de atividades e tarefas que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

Este documento estabelece um plano de ação contendo o processo de gestão de riscos para a área de TI de forma a orientar a identificação, a análise, a avaliação, o tratamento, a priorização, o monitoramento e a comunicação dos riscos inerentes aos recursos, serviços e sistemas informatizados do IFTO.

Para que o objetivo geral seja alcançado, foram definidos os seguintes objetivos específicos:

- Definir as atividades e tarefas que compõem o processo de gestão de riscos;
- Definir as técnicas e ferramentas para identificação, análise, avaliação, tratamento, monitoramento e comunicação de riscos para a área de TI do IFTO;
- Definir os papéis e responsabilidades de cada envolvido na gestão de riscos.

#### 1.2. Escopo e abrangência

O Plano de Gestão de Riscos em Tecnologia da Informação proposto neste documento permeia todo o ciclo de vida das iniciativas para desenvolvimento, implementação e gestão de soluções que envolvem as áreas de Tecnologia da Informação do IFTO. Abrange as áreas de infraestrutura de TI, manutenção de equipamentos de TI, suporte operacional, desenvolvimento de sistemas, governança e gestão de TI, redes e segurança da informação.

#### 1.3. Termos, definições, acrônimos e abreviações

Neste documento são utilizados diversos termos referentes a gestão de riscos de forma geral. O Quadro 1 apresenta as definições, os acrônimos e as abreviações de forma a facilitar a compreensão.

Quadro 1 – Definições, acrônimos e abreviações

Termos, Acrônimos e Abreviações	Definição
Ameaça	Causa potencial de um incidente indesejado, que possui potencial para comprometer ativos através de exploração de

	vulnerabilidades (SISP, 2016).
Ativos da Informação	Os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso (BRASIL, 2013).
Consequência	Resultado de um evento que afeta os objetivos (ISO, 2018).
Controle	Medida que mantém e/ou modifica o risco (ISO, 2018).
Evento	Ocorrência ou mudança em um conjunto específico de circunstâncias (ISO, 2018).
Gestão de Riscos	Atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos (ISO, 2018).
Probabilidade	Chance de algo acontecer (ISO, 2018)
Risco	Efeito da incerteza nos objetivos. Pode ser positivo, negativo ou ambos, e pode abordar, criar e resultar em oportunidades e ameaças (ISO, 2018).
TI	Tecnologia da Informação.
Stakeholder (parte interessada)	Pessoa ou organização que pode afetar, ser afetada ou perceber-se afetada por uma decisão ou atividade (ISO, 2018).
Vulnerabilidade	Fraqueza de um determinado ativo ou controle que pode ser explorado por uma ameaça (SISP, 2016).

#### 1.4. Referências

As referências para a construção do Plano de Gestão de Riscos em Tecnologia da Informação são:

1. Metodologia de Gestão de Riscos do IFTO (2015).
2. Instrução Normativa Complementar DSIC/GSI/PR nº 4, de 15 de fevereiro de 2013.
3. Instrução Normativa Conjunta PR/CGU nº 1, de 10 de maio de 2016.
4. Norma Técnica ABNT NBR ISO 31000: 2018 *Risk management: guidelines, provides principles, framework and a process for managing risk.*
5. Norma Técnica ABNT 31010:2019. *Risk Management: Risk assessment techniques.*

#### 1.5. Vigência

O Plano de Gestão de Riscos em Tecnologia da Informação tem vigência para o período de 2020 a 2024.

## 2. RISCOS DE TECNOLOGIA DA INFORMAÇÃO

Vários são os riscos que afetam as áreas de Tecnologia da Informação. O Quadro 2 apresenta o resumo de alguns riscos relacionados à área de TI que serão tratados pelo Plano de Gestão de Riscos em Tecnologia da Informação.

Quadro 2 – Riscos, causas e consequências

Risco	Causa	Consequência	Controle
Falha humana relacionada ao manuseio do grupo gerador de energia secundária.	Acidente ao manusear equipamentos ou abastecimento do tanque de combustível.	Interrupção no fornecimento de energia secundária para o Data Center.	Capacitação.
Acesso físico não autorizado (indevido) a sala de equipamentos de rede.	Falhas dos controles de acesso físico ao Data Center.	Indisponibilidade de recursos, serviços e sistemas informatizados. Roubo de informações.	Controle de Acesso Físico.
Interrupção de energia elétrica.	Fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 24 horas. Fator interno que comprometa a rede elétrica do prédio com curto-circuitos, incêndios e infiltrações.	Indisponibilidade de recursos, serviços e sistemas informatizados. Roubo de informações.	Grupo Gerador.
Falhas ou queima de componentes eletrônicos.	Tempestades Atmosféricas. Oscilações Elétricas.	Indisponibilidade de recursos, serviços e sistemas informatizados. Perda de informações.	Equipamentos Redundantes.
Oscilações ou quedas na comunicação de dados entre a Reitoria e os campi	Interrupção de fornecimento de energia. Oscilações de Energia. Falha humana.	Indisponibilidade de recursos, serviços e sistemas informatizados. Perda de informações.	Grupo Gerador. Link Redundante.

Indisponibilidade de <i>backups</i> de dados.	Cópia de segurança dos dados não disponível ou sem integridade em razão de indisponibilidade de rede, quedas ou oscilações de energia ou erros de configuração das estratégias de <i>backups</i> .	Não recuperação de dados.	Estratégias de <i>backup</i> e restauração de dados.
Falhas na restauração de dados.	Erros de rede. Quedas ou oscilações de energia. Erros de configuração das estratégias de <i>backups</i> .	Não recuperação de dados. Perda de dados.	Estratégias de <i>backup</i> e restauração de dados.
Indisponibilidade de <i>link</i> de internet redundante.	Inexistência de contrato de prestação de serviços de internet para <i>link backup</i> .	Indisponibilidade de recursos, serviços e sistemas informatizados.	Contrato de <i>link</i> redundante de internet.
Bloqueio ou dificuldades de acesso físico ao Data Center em razão de desastres naturais.	Alagamento. Desabamento. Incêndio. Infiltrações decorrentes de águas da chuva e ventanias após evento de destelhamento. Problemas decorrentes de vazamento de água potável, como é o caso do hidrante na parede ao lado do Data Center. Drenos dos equipamentos condensadores de ar-condicionado entupidos, causando inundação no piso elevado ou em cima dos equipamentos. Inundação causada por evento de chuvas que podem comprometer sistemas pluviais internos de escoamento de águas.	Indisponibilidade de recursos, serviços e sistemas informatizados. Perda de dados.	Sistemas de Proteção contra raios, alagamentos e incêndios.
Equipamentos de climatização da sala do Data Center com mau funcionamento.	Variação de temperatura.	Queima de componentes eletrônicos. Indisponibilidade de recursos, serviços e sistemas informatizados.	Sistema de automação de ar-condicionado redundante.
Falhas no acesso ao <i>storage</i> de dados	Indisponibilidade de rede de comunicação de dados. Oscilações de energia elétrica. Procedimento incorreto de acesso ao <i>storage</i> . Procedimento incorreto de configuração do <i>storage</i> .	Indisponibilidade de recursos, serviços e sistemas informatizados.	Equipamentos Redundantes. Grupo Gerador. Capacitações.
Falha ou indisponibilidade do sistema unificado de autenticação de usuários.	Indisponibilidade de rede de comunicação de dados. Oscilações ou quedas de energia elétrica. Procedimento incorreto no sistema de autenticação unificado.	Indisponibilidade de recursos, serviços e sistemas informatizados.	Equipamentos Redundantes. Grupo Gerador. Capacitações.
Falhas na disponibilidade de rede lógica de dados do <i>Campus/Reitoria</i> .	Erros de configuração de ativos de rede. Quedas ou oscilações de energia elétrica. Queima ou falhas de componentes eletrônicos. Falta de conhecimento sobre manutenção preventiva e corretiva em cabeamento estruturado. Ausência de capacitações em redes de comunicação de dados.	Indisponibilidade de recursos, serviços e sistemas informatizados.	Equipamentos Redundantes. Grupo Gerador. Capacitações.
Falhas ou erros no acesso a sistema ou banco de dados.	Inexistência de conectividade de rede. Falhas ou erros na configuração do serviço. Comprometimento do sistema operacional. Ataques internos e externos.	Indisponibilidade de sistemas informatizados. Perda de dados.	Equipamentos Redundantes. Grupo Gerador. Capacitações.

Fonte: Diretoria de Tecnologia da Informação

### 3. METODOLOGIA

A metodologia para construção deste Plano baseia-se nas ferramentas de gestão conhecidas por Ciclo de Deming, para melhoria contínua de processos e produtos (PDCA), e a ferramenta para construção de plano de ação 5W2H. O Quadro 3 apresenta as fases da metodologia utilizada para a construção deste documento.

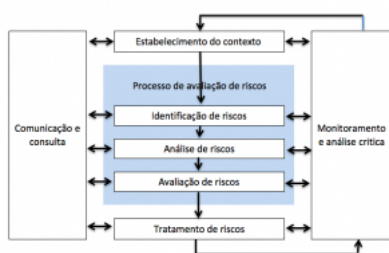
Fase	Atividades
Planejamento	Planejar o processo de gestão de riscos com suas atividades, tarefas, ferramentas e técnicas.
Desenvolvimento	Definir papéis e responsabilidades bem como as atividades e tarefas a serem executadas por cada papel.
Checkagem	Definir como será o monitoramento e o controle do plano de ação a ser seguido.
Ação	Comunicar o cronograma para a execução do plano.

#### 4. PROCESSO DE GESTÃO DE RISCOS

Segundo o TCU (2018b), o processo de gestão de riscos envolve a identificação, a análise e a avaliação de riscos, a seleção e a implementação de respostas aos riscos avaliados, o monitoramento de riscos e controles, e a comunicação sobre riscos com partes interessadas, internas e externas. Esse processo é aplicado a uma ampla gama das atividades da organização, em todos os níveis, incluindo estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos, e é suportado pela cultura e pela estrutura de gestão de riscos da entidade.

A estrutura de gestão de riscos adotada pela área de TI utiliza o modelo de gerenciamento de riscos proposto pelo IFTO (2015) com uso das atividades apresentadas pela norma ISO 31000 (2018). Além disso, observa as recomendações do TCU (2018b) e da CGU (2018), e está em conformidade com a Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016 (BRASIL, 2016). O processo de gerenciamento de riscos é composto por cinco atividades, conforme demonstra a Figura 1.

Figura 1 – Processo de Gestão de Riscos de TI do IFTO



Fonte: Norma ISO 31000 (2018)

A Figura 1 apresenta as atividades executadas para a realização da gestão de riscos relacionados aos projetos de TI. São elas: estabelecimento do contexto, processo de avaliação de riscos (identificação de riscos, análise de riscos e avaliação de riscos), tratamento de riscos, monitoramento e análise crítica, e comunicação e consulta com as partes interessadas. As próximas seções detalham as atividades e tarefas a serem realizadas pela equipe de TI.

##### 4.1. Estabelecimento do Contexto

A atividade de estabelecimento do contexto para a gestão de riscos na área de TI do IFTO adota a metodologia de gestão de riscos do IFTO (2015) e a estrutura do modelo de gestão de riscos proposto pela Instrução Normativa Conjunta MP/CGU nº 1/2016 (BRASIL, 2016). Nesta atividade são considerados:

a) **ambiente interno:** inclui, entre outros elementos, integridade, valores éticos e competência das pessoas, maneira pela qual a gestão delega autoridade e responsabilidades, estrutura de governança organizacional e políticas e práticas de recursos humanos. O ambiente interno é a base para todos os outros componentes da estrutura de gestão de riscos, provendo disciplina e prontidão para a gestão de riscos;

b) **fixação de objetivos:** a Diretoria de TI juntamente com o Comitê Gestor de TI definem os objetivos estratégicos da área de TI e os comunica. Os objetivos estão alinhados à missão e à visão da organização de forma que a identificação de riscos é realizada potencialmente impedindo que o risco prejudique o cumprimento da missão institucional. Nesta atividade são realizados quatro tarefas recomendadas pelo TCU (2018a):

1. Identificar quais objetivos, premissas, restrições ou resultados devem ser alcançados.
2. Identificar os processos de trabalho relevantes para o alcance dos objetivos/resultados.
3. Identificar as pessoas envolvidas nesses processos e especialistas na área.
4. Mapear os principais fatores internos e externos que podem afetar o alcance dos objetivos/resultados (pessoas, sistemas informatizados, estruturas organizacionais, legislação, recursos, *stakeholders* etc).

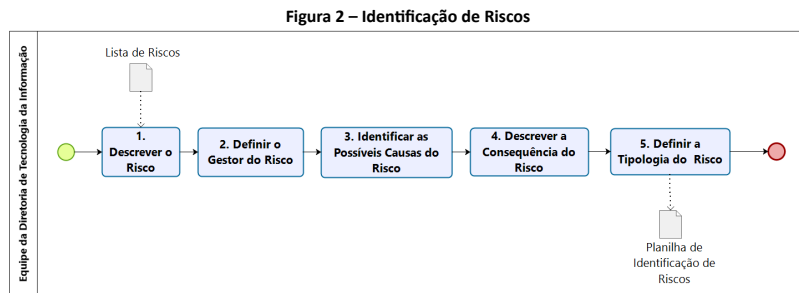
Segundo a metodologia de gestão de riscos adotada pelo IFTO (2015), esta atividade tem por objetivo identificar por meio de *workshop* e *brainstorming* os processos críticos sujeitos a vulnerabilidades de forma que os riscos possam ser gerenciados.

##### 4.2. Processo de Avaliação de Riscos

O processo de avaliação de riscos é composto por identificação, análise e avaliação de riscos.

#### 4.2.1. Identificação de Riscos

Segundo a norma ISO 31000 (2018), a identificação de riscos contempla a busca, o reconhecimento e a descrição de eventos que podem afetar objetivos, as fontes que possam originar tais eventos, e as possíveis causas e consequências. Para a identificação de riscos, são realizadas cinco tarefas conforme demonstra a Figura 2.



Fonte: Diretoria de Tecnologia da Informação (IFTO)

A Figura 2 apresenta a atividade Identificação de riscos com suas tarefas: descrever o risco, definir o gestor do risco, identificar as possíveis causas do risco, descrever a consequência do risco e definir a tipologia de risco. Esta atividade inicia-se com um lista de riscos gerada por meio de técnicas de *brainstorming*, listas de verificação (*checklists*), entrevistas estruturadas e semiestruturadas e questionários, e se encerra com a entrega do inventário de riscos em uma planilha de identificação de riscos.

Para identificar riscos, são considerados os contextos interno e externo em que o processo de TI está inserido, a fim de definir as providências específicas para um risco oriundo de um objetivo estratégico, projeto ou atividade. Para descrever o risco é utilizado como padrão: "Devido a <causa ou o fator de risco = fonte+vulnerabilidade>, poderá acontecer <evento>, o que poderá levar a <consequência> impactando no/na <dimensão do objetivo de TI>".

Os tipos de riscos de TI serão categorizados de acordo com a Instrução Normativa Conjunta MP/CGU nº 1/2016. A definição da categoria do risco permite o conhecimento e a análise crítica dos riscos de TI e contribuem para maior objetividade das análises quanto aos impactos. O Quadro 4 apresenta a taxonomia de riscos utilizada para a identificação e análise de riscos.

**Quadro 4 – Tipologia de Riscos**

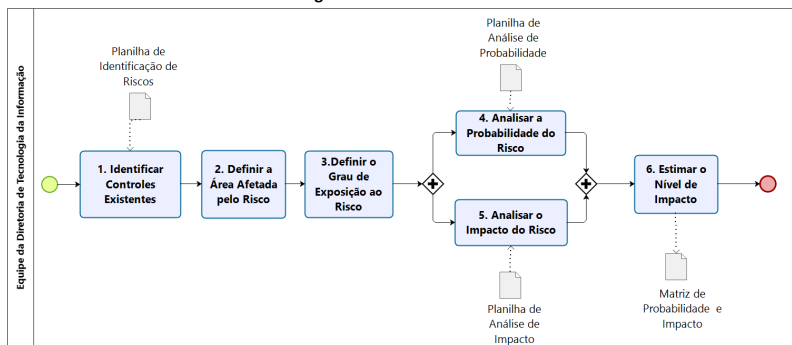
Tipo/Categoria	Descrição
Operacionais	Eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas.
Imagem/Reputação	Eventos que podem comprometer a confiança da sociedade em relação à capacidade da instituição em cumprir sua missão institucional.
Legais	Eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade.
Financeiro/Orçamento	Eventos que podem comprometer a capacidade da instituição de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações.

Fonte: Instrução Normativa Conjunta MP/CGU nº 1/2016 (BRASIL, 2016)

#### 4.2.2. Análise de Riscos

Refere-se ao desenvolvimento da compreensão sobre o risco e à determinação do nível de impacto do risco. Esta atividade é responsável por compreender, criticar e estimar o nível de criticidade de cada risco, determinado com base na probabilidade (chance de ocorrer) e no impacto (consequências) sobre um ou mais objetivos do processo. A Figura 3 apresenta as seis tarefas a serem realizadas para fazer a análise de riscos.

Figura 3 – Análise de Riscos



Fonte: Diretoria de Tecnologia da Informação (IFTO)

Conforme demonstra a Figura 3, a análise de riscos inicia-se com a identificação dos controles existentes para os riscos apresentados. Em seguida, define-se a área afetada e o grau de exposição ao risco. Depois é feita a análise de probabilidade e impacto e, por fim, é estimado o nível de impacto. A análise de riscos é realizada de forma quantitativa e qualitativa.

**a) Análise Qualitativa de Riscos:** avalia a exposição ao risco priorizando os riscos que serão objetos de análise ou ação adicional. A análise qualitativa dos riscos será feita a partir da definição de escalas de probabilidade e impacto através da técnica de matriz de probabilidade e consequência.

Na análise dos riscos são definidos os tipos de controle para cada risco de acordo com o nível de maturidade da instituição em relação ao controle a ser adotado. Os tipos de controle são: corretivo, detectivo e preventivo.

Controle corretivo apresenta medidas que podem ser executadas quando um risco já foi causado. O controle detectivo visa à identificação de um erro ou irregularidade depois que este tenha ocorrido. Já o controle preventivo diz respeito a levantar quais ações podem ser realizadas visando à prevenção de possíveis causas de riscos (intencionais ou não). O Quadro 5 apresenta os tipos de controle com o nível de maturidade e probabilidade de ocorrência do risco. A escala foi adaptada de PMI (2013).

Quadro 5 – Escala de Tipos de Controle de Risco

Tipo de Controle	Nível de Maturidade	Probabilidade de ocorrer o risco
Corretivo	Inexistente	Elevada
	Fraco	Muito Alta
Detectivo	Insatisfatório	Alta
Preventivo	Satisfatório	Média
	Forte	Baixa

Fonte: Adaptado (PMI, 2013)

A partir da definição do tipo de controle a ser aplicado para cada risco de acordo com a escala estabelecida no Quadro 5, é feita a avaliação de forma a verificar o nível de controle a ser adotado. Para realizar essa atividade são utilizadas as recomendações contidas no Manual de gestão de riscos divulgado pelo TCU e publicado em 2018 (TCU, 2018).

Para analisar riscos é utilizada a matriz de probabilidade e impacto, baseada nas publicações do TCU (2018a) e da CGU (2018). A matriz define o nível de riscos a partir da combinação das escalas de probabilidade e de impacto.

A probabilidade consiste no resultado da materialização de um dado risco em determinado horizonte de tempo. É a chance de o evento ocorrer dentro do prazo previsto para se alcançar o objetivo/resultado. Por exemplo, se o objeto da gestão de riscos é uma aquisição de computadores, estima-se a probabilidade da ocorrência do risco durante o prazo previsto para entrega do seu produto final.

As escalas podem variar de acordo com o objeto de gestão e com o grau de precisão na definição dos níveis de probabilidade. Na análise de riscos são utilizadas escalas qualitativas de probabilidade com amplitude de até cinco níveis: baixa, média, alta, muito alta e elevada.

O cálculo da probabilidade deverá ser feito a partir da média aritmética entre os seis macro fatores de riscos (TI, RH, Processos, Organização, Legislação, Comunicação) acrescidos da exposição ao risco (elevada, muito alta, alta, média e baixa). Então, obtém-se um número para a classificação da probabilidade do risco (baixa, média, alta, muito alta e elevada), para cada risco identificado, conforme demonstra o Quadro 6. Esta escala foi adaptada de TCU (2018b).

Quadro 6 – Escala de Probabilidade de Ocorrência do Risco

Probabilidade	Descrição	Peso
Baixa	<b>Improvável.</b> Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	<=20
Média	<b>Rara.</b> De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	<=40
Alta	<b>Possível.</b> De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	<=60
Muito Alta	<b>Provável.</b> De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	<=75

Elevada	<b>Praticamente certa.</b> De forma inequívoca, o evento ocorrerá. As circunstâncias indicam claramente essa possibilidade.	>75
---------	---	-----

Fonte: Diretoria de Tecnologia da Informação adaptado de TCU (2018b)

O Quadro 6 apresenta a escala de probabilidade definida de forma quantitativa de acordo com o peso definido. O cálculo do impacto consiste no resultado da materialização de um dado risco, medido por critérios preferencialmente quantitativos. A avaliação do impacto deverá ser feita a partir da média ponderada entre as áreas afetadas: imagem, financeiro, legislação e operacional.

De acordo com os valores informados nas categorias (imagem, financeiro, legislação e operacional), será realizada uma média que define o nível de impacto do risco para a fase da aquisição de TI. Com isso, obtém-se o número indicativo do nível de impacto (baixo, médio, alto, muito alto e elevado) para cada risco identificado.

A avaliação da relevância do impacto dos riscos deverá ser realizada através da relevância do impacto em cada área (imagem, financeiro, legislação e operacional), conferindo uma nota ao impacto. Essa nota poderá se abrandar ou se agravar de acordo com o nível de tolerância (tempo) à ação saneadora.

A Diretoria de Tecnologia da Informação (DTI) optou por definir uma escala adaptada do referencial básico de gestão de riscos do TCU (2018b) para realizar o cálculo do nível de impacto. O impacto varia de acordo com a área impactada. Quando um risco impactar mais de uma área, deverá ser usada a área mais impactada.

Esse cálculo é realizado para definir o nível de tolerância a riscos. De acordo com o valor atribuído ao peso é definido o impacto do risco. O Quadro 7 apresenta a definição dos pesos adotados para cálculo de impacto de riscos. A escala de impacto é definida em muito baixo (1), baixo (2), médio (3), alto (4) e muito alto (5).

**Quadro 7 – Escala de Impacto do Risco**

Impacto	Descrição	Peso
Muito baixo (1)	Mínimo impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade).	<=1.5
Baixo (2)	Pequeno impacto nos objetivos.	<= 2.5
Médio (3)	Moderado impacto nos objetivos, porém, recuperável.	<= 3.5
Alto (4)	Significativo impacto nos objetivos, de difícil reversão.	< = 4.5
Muito Alto (5)	Catastrófico impacto nos objetivos (idem), de forma irreversível.	> 4.5

Fonte: Diretoria de Tecnologia da Informação adaptado de TCU (2018b)

O Quadro 8 apresenta a pontuação de impacto. A pontuação é definida de acordo com as áreas da organização. Os pesos foram definidos de acordo com o nível de tolerância para o risco. A pontuação de impacto leva em conta a escala definida pelo IFTO (2015).

**Quadro 8 – Pontuação para Escala de Impacto do Risco**

Pontuação	Escala				
	Imagem	Financeiro	Legislação	Operacional	Nível de Tolerância
5	De caráter internacional	Massivo	Perturbações muito graves	Perturbações muito graves	Muito alto
4	De caráter nacional	Severo	Graves	Graves	Alto
3	Regional	Moderado	Limitadas	Limitadas	Médio
2	Local	Leve	Leves	Leves	Baixo
1	De caráter individual	Insignificante	Muito leves	Muito leves	Muito baixo

Fonte: IFTO (2015)

A pontuação apresentada no Quadro 8 leva em consideração o nível de tolerância. O resultado da avaliação dos riscos entre probabilidade *versus* impacto de sua ocorrência é representado através da matriz de riscos. Os riscos possuem limites de exposição. Para apresentar os limites foi realizada uma adaptação da convenção apresentada pelo TCU (2018a) no Quadro 9.

**Quadro 9 – Faixas de Nível de Risco**

Faixa	Nível
Vermelha	Muito alto (Transferir) – altíssima exposição
Laranja	Alto (Evitar) – alta exposição
Amarela	Médio (Mitigar) – média exposição (monitorar)
Verde	Baixo e muito baixo (Aceitar) – baixa exposição

Fonte: Diretoria de Tecnologia da Informação adaptado do TCU (2018a)

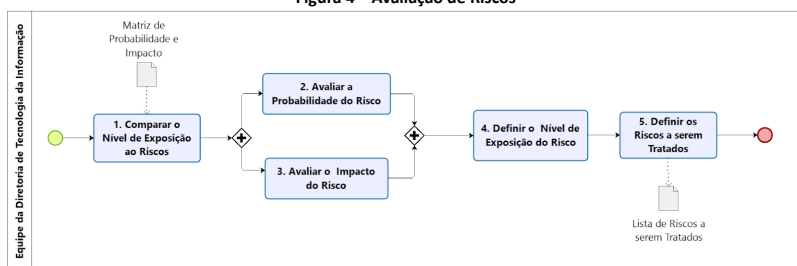
Os níveis de riscos identificados são posicionados na matriz de riscos de acordo com a avaliação realizada de probabilidade de ocorrência e impacto.

**b) Análise Quantitativa de Riscos:** efetua a análise numérica do efeito dos riscos identificados. A análise quantitativa de riscos é realizada através da ferramenta mapa de riscos presente na planilha documentadora denominada Mapa de Gerenciamento de Riscos.

### 4.2.3. Avaliação de Riscos

Envolve a comparação do seu nível com o limite de exposição a riscos, a fim de determinar se o risco é aceitável. O propósito da avaliação de riscos envolve a comparação dos resultados da análise de riscos com os critérios de riscos estabelecidos para determinar onde é necessária ação adicional. Os riscos são avaliados sob a perspectiva de probabilidade e impacto de sua ocorrência. A avaliação de riscos é realizada por meio de análises qualitativas. O limite de exposição a riscos representa o nível de risco acima do qual é desejável o tratamento do risco. Os riscos são avaliados quanto à sua condição de inerentes e residuais. A atividade de avaliação possui cinco tarefas conforme apresenta a Figura 4.

Figura 4 – Avaliação de Riscos



Fonte: Diretoria de Tecnologia da Informação (IFTO)

Conforme se verifica na Figura 4, a avaliação de riscos é realizada através da avaliação de probabilidade e impacto do risco de forma que possam ser definidos pelo gestor de riscos quais são os riscos a serem tratados. Os níveis de riscos identificados são posicionados na matriz de acordo com a avaliação realizada de probabilidade de ocorrência e impacto.

A avaliação de relevância do impacto utiliza os critérios: imagem, financeiro, legislação e operacional, conferindo uma nota ao impacto conforme determina a metodologia de gestão de riscos do IFTO (2015). Os níveis de impacto podem ser: massivo, severo, moderado e leve. A criticidade de vulnerabilidade será: crítico, moderado e leve.

Após identificação e avaliação de riscos, sua priorização se dará pela maior relação entre impacto e probabilidade, estabelecendo assim o grau de exposição ao risco e que orientará a prioridade de acompanhamento periódico. A Figura 5 apresenta a matriz de probabilidade e impacto utilizada pela DTI. A matriz de riscos é uma adaptação de MPDG (2016), CGU (2018) e TCU (2018b).

Figura 5 – Matriz de Probabilidade e Impacto

P R O B A B I L I D A D E	Elevada			2		3	
	Muito Alta				1	11	
	Alta			4	10	8	
	Média			6	16	15	
	Baixa				3	12	
		Muito Baixo	Baixo	Medio	Alto	Muito Alto	
		IMPACTO					

Transferir  
Nível Muito Alto

Evitar  
Nível Alto

Mitigar  
Nível Médio

Aceitar  
Nível Baixo  
Nível Muito Baixo

Riscos

Fonte: Diretoria de Tecnologia da Informação adaptado de MPDG (2016), CGU (2018) e TCU (2018b)

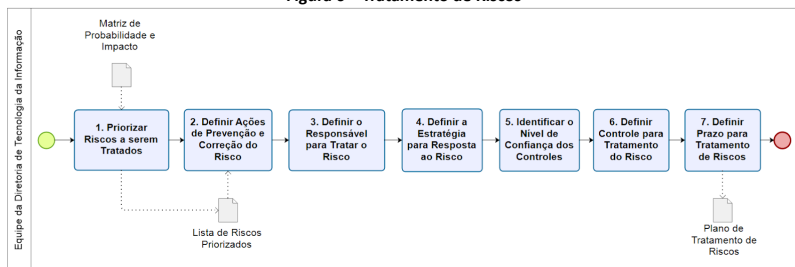
Uma vez que os riscos foram identificados e avaliados de acordo com a matriz de probabilidade e impacto (Figura 5), a atividade subsequente é a priorização dos riscos para o tratamento. A priorização de riscos é feita a partir do cálculo de nível de impacto. Nessa atividade são definidas atitudes perante os riscos a serem tratados de acordo com o nível de impacto para o processo.

### 4.3. Tratamento de Riscos

O tratamento de riscos compreende o planejamento e a realização de ações para modificar o nível do risco. O nível do risco pode ser modificado por meio de medidas de resposta ao risco que mitiguem, transfiram ou evitem esses riscos. Para tratar os riscos são definidas estratégias: evitar, transferir, aceitar ou mitigar. A escolha da estratégia dependerá do nível de exposição a riscos previamente estabelecido pela organização em confronto com a avaliação que se fez do risco. A atividade de tratamento dos riscos possui sete tarefas, conforme demonstra a Figura 6.



Figura 6 – Tratamento de Riscos



Fonte: Diretoria de Tecnologia da Informação (IFTO)

De acordo com a Figura 6, o tratamento de riscos se inicia com a priorização de riscos apresentados na matriz de probabilidade e impacto. Em seguida, são definidas as ações de prevenção, detecção e correção dos riscos, o responsável para tratar o risco, a resposta para o risco e o controle para tratamento do risco. Por fim, é construído o plano de ação para tratamento do risco.

**a) Planejar as Respostas a Riscos:** no planejamento de resposta a riscos deverão ser desenvolvidas opções e ações para aumentar as oportunidades e reduzir as ameaças relacionadas aos objetivos estratégicos de TI. Os riscos deverão ser tratados através de um plano de ação que utiliza a ferramenta 5W2H para definir as ações de contingência. Para definir as estratégias de respostas são adotadas as recomendações do PMBOK (PMI, 2013).

**b) Estratégias para Riscos Negativos ou Ameaças:** para tratar os riscos negativos ou ameaças deverão ser utilizadas as estratégias: evitar ou eliminar, transferir, mitigar e aceitar, conforme mostra o Quadro 10. Estas estratégias são adaptadas de CGU (2018).

Quadro 10 – Estratégia para Riscos Negativos ou Ameaças

Estratégia	Descrição
Evitar/Eliminar (Alto)	Um risco normalmente é evitado quando é classificado como “Alto” ou “Extremo”, e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco. Evitar o risco significa encerrar o processo organizacional. Nesse caso, essa opção deve ser aprovada pelo Comitê de Gestão Estratégica. (CGU, 2018)
Transferir (Muito Alto)	Transfere um risco para terceiro, transferindo os impactos e a responsabilidade. Passa a responsabilidade e impactos do risco para uma terceira parte, geralmente na forma de subcontratação. Um risco transferido não é eliminado, este ainda poderá se materializar e, por isso, deve ser monitorado.
Mitigar (Alto)	Um risco normalmente é mitigado quando é classificado como “Alto” ou “Extremo”. A implementação de controles, neste caso, apresenta um custo/benefício adequado. Mitigar o risco significa implementar controles que possam diminuir as causas ou as consequências dos riscos, identificadas na etapa de Identificação e Análise de Riscos (CGU, 2018).
Aceitar (Baixo)	Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco (CGU, 2018).

Fonte: Diretoria de Planejamento e Desenvolvimento Institucional CGU (2018)

**c) Estratégias para Riscos Positivos ou Oportunidades:** para tratar os riscos positivos ou oportunidades deverão ser utilizadas as estratégias: explorar, compartilhar, melhorar e aceitar. O Quadro 11 apresenta as estratégias definidas para a área de TI do IFTO.

Quadro 11 – Estratégia para Riscos Positivos ou Oportunidades

Estratégia	Descrição
Explorar	Muda-se a estratégia para garantir que a oportunidade seja aproveitada. Garante que a oportunidade ocorra para explorar seus benefícios. Procura eliminar a incerteza associando ao risco positivo, adicionando trabalho ou mudando o projeto para assegurar que a oportunidade ocorra.
Compartilhar	Um risco normalmente é compartilhado quando é classificado como “Alto” ou “Extremo”, mas a implementação de controles não apresenta um custo/benefício adequado. Pode-se compartilhar o risco por meio de terceirização ou apólice de seguro, por exemplo (CGU, 2018).
Melhorar	Aumenta a probabilidade e/ou impacto de uma oportunidade. São tomadas ações proativas para que as chances (probabilidade) ou o impacto positivo sejam aumentados. Identificar os principais causadores desses riscos positivos ajuda a aumentar a probabilidade de ocorrência.
Aceitar	Tira proveito caso a oportunidade ocorra. A aceitação ativa envolve a criação de planos de contingências para serem implementados se os riscos ocorrerem. A aceitação passiva deixa que as ações sejam determinadas quando e se os riscos ocorrerem.

Fonte: Diretoria de Tecnologia da Informação adaptado de CGU (2018) e TCU (2018a)

**d) Níveis de Confiança dos Controles:** deverão ser definidos os controles para a gestão de riscos de acordo com o nível de confiança existente. Este Plano recomenda o uso da escala definida pela Controladoria-Geral da União (CGU, 2018) e pelo Tribunal de Contas da União

(TCU, 2018c). O Quadro 12 apresenta os níveis de confiança dos controles adotados pela área de TI no IFTO.

Quadro 12 – Níveis de Confiança dos Controles

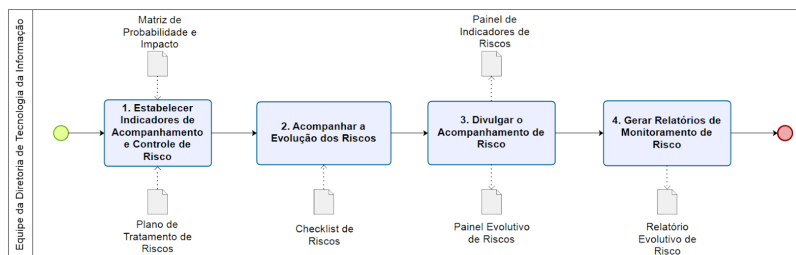
Nível de Confiança	Controle
Inexistente	Nenhum nível de confiança. Controles inexistentes, mal desenhados ou mal implementados.
Fraco	Nível de confiança de 20%. Controles têm abordagens <i>ad hoc</i> , tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.
Mediano	Nível de confiança de 40%. Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.
Satisfatório	Nível de confiança de 60%. Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.
Forte	Nível de confiança de 80%. Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco.

Fonte: TCU (2018c)

#### 4.4. Monitoramento e Análise Crítica

Compreende o acompanhamento e a verificação do desempenho ou da situação de elementos da gestão de riscos, podendo abranger a política, as atividades, os riscos, os planos de tratamento de riscos, os controles e outros assuntos de interesse. Tem como objetivo avaliar a qualidade da gestão de riscos e dos controles internos da gestão, por meio de atividades gerenciais contínuas e/ou avaliações independentes, buscando assegurar que estes funcionem como previsto e que sejam modificados apropriadamente, de acordo com mudanças nas condições que alterem o nível de exposição a riscos. A Figura 7 apresenta as quatro tarefas a serem realizadas para monitoramento e análise crítica de riscos.

Figura 7 – Monitoramento e Análise Crítica



Fonte: Diretoria de Tecnologia da Informação (IFTO)

A atividade de monitoramento das ações de tratamento de riscos apresentada na Figura 7 deverá envolver a verificação contínua ou periódica do funcionamento da implementação e dos resultados das medidas mitigadoras. Considera o tempo necessário para que as medidas mitigadoras produzam seus efeitos. Esta atividade é parte integrante do processo de gestão e de tomada de decisão e acompanha o ciclo de planejamento institucional.

As tarefas de controle deverão ser realizadas através de procedimentos estabelecidos e executados para mitigar os riscos definidos para realizar o tratamento dos riscos. Elas deverão ser executadas através de controles internos de gestão preventivos e detectivos, através do plano de tratamento de riscos, juntamente com listas de verificação.

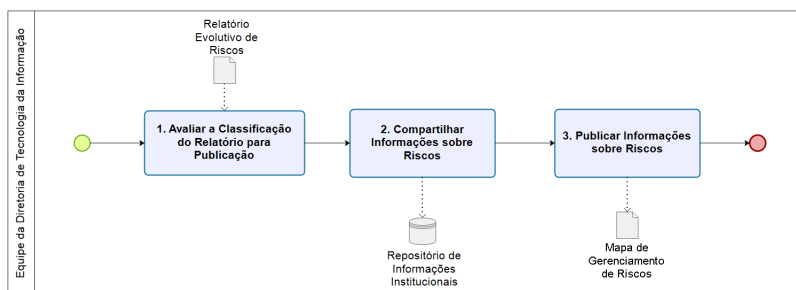
O Plano de Gestão de Riscos de Tecnologia da Informação deverá ter acompanhamento sistemático, sendo reavaliado semestralmente e, nos casos em que o diretor de TI em conjunto com sua equipe de apoio julguem necessário, esse prazo pode ser redimensionado.

A atividade de monitoramento e controle de riscos deverá ser realizada durante reuniões semestrais de planejamento de TI. Durante as reuniões, devem ser avaliadas as modificações dos atributos de situação, probabilidade de ocorrência e impacto dos riscos, bem como os valores para os gatilhos e a efetividade dos planos de resposta para cada um dos riscos.

#### 4.5. Comunicação e Consulta

A atividade de comunicação e consulta refere-se à identificação das partes interessadas e ao compartilhamento de informações relativas à gestão de riscos sobre determinado objeto, observada a classificação da informação quanto ao sigilo. Esta atividade fornece as informações relativas ao risco e ao seu tratamento para todos aqueles que possam influenciar ou ser influenciados por esse risco, sob pena de ele se materializar plenamente. A Figura 8 apresenta as três tarefas que compõem o fluxo de procedimentos realizados por esta atividade.

Figura 8 – Comunicação e Consulta



Fonte: Diretoria de Tecnologia da Informação (IFTO)

Conforme apresenta a Figura 8, a comunicação e consulta deverá se iniciar a partir da entrega do relatório evolutivo de riscos. Em seguida, será definida qual será a forma de publicação e compartilhamento da informação através do repositório sobre riscos. O mapa de gerenciamento de riscos deverá ser publicado para que todos os setores do IFTO possam compreender os riscos inerentes ao setor de TI.

#### 4.5.1. Documento para a Gestão de Riscos em TI

O documento adotado para padronização de riscos é denominado de Mapa de Gerenciamento de Riscos, que deverá ser utilizado pelo gestor de risco (diretor de TI) para realizar a gestão de riscos em todos os macroprocessos definidos para a área de TI. O Quadro 13 apresenta a síntese das planilhas existentes no Mapa de Gerenciamento de Riscos.

Quadro 13 – Mapeamento de Gerenciamento de Riscos

Artefato	Descrição	Técnicas
Planilha de Identificação de Riscos	Identifica riscos relacionados à área de TI.	<i>Brainstorming;</i> entrevistas estruturadas ou semiestruturadas; <i>checklists</i>
Planilha de Análise de Probabilidade	Calcula a probabilidade de o risco ocorrer.	Matriz de Probabilidade e Consequência
Análise de Impacto	Calcula o impacto do risco, caso o risco ocorra.	Matriz de Probabilidade e Consequência
Mapa de Calor	Avalia o nível de exposição do risco.	Matriz de Probabilidade e Consequência
Plano de Ação	Define resposta para o risco de acordo com a estratégia definida.	5W2H

Fonte: Diretoria de Tecnologia da Informação (IFTO)

## 5. PAPÉIS E RESPONSABILIDADES

Para realizar a gestão de riscos na área de TI, serão definidos papéis e responsabilidades, conforme apresenta o Quadro 14.

Quadro 14 – Papéis e Responsabilidades

Papel	Responsabilidade
Comitê Gestor de TI	- Aprovar o Plano de Gestão de Riscos em Tecnologia da Informação.
Comitê Gestor de Segurança da Informação	- Aprovar o Plano de Gestão de Riscos em Tecnologia da Informação.
Diretoria de Tecnologia da Informação	- Associar um agente responsável para cada risco mapeado e avaliado, formalmente identificado nos projetos ou projetos de contingência e resposta aos riscos. - Assegurar que o risco seja gerenciado de acordo com as diretrizes estabelecidas neste documento. - Garantir que as informações adequadas sobre o risco estejam disponíveis e atualizadas. - Gerenciar e reportar informações adequadas sobre o gerenciamento de riscos.
Gestor de Riscos	- Realizar identificação e avaliação de riscos no âmbito das atividades desenvolvidas pela área de Tecnologia da Informação. - Elaborar e manter atualizado o Mapa de Gerenciamento de Riscos de TI e o plano de ação para tratamento de riscos. - Monitorar o risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados, de acordo com a política de gestão de riscos. - Atuar na primeira linha de defesa, com a implementação de ações corretivas para resolver deficiências nos mapas e nos planos de ação de riscos. - Manter controles eficazes e conduzir procedimentos de resposta aos riscos. - Observar a inovação e a adoção de boas práticas no gerenciamento de riscos de TI.

## 6. TÉCNICAS PARA GESTÃO DE RISCOS

As técnicas usadas para realizar a gestão de riscos de TI no IFTO são recomendadas pela ISO 31010 (2019). Para cada atividade de administração de riscos podem ser utilizadas várias ferramentas. O Quadro 15 apresenta as ferramentas usadas para gerenciar riscos na área de TI.

Quadro 15 – Técnicas utilizadas para gestão de riscos

Técnicas	Descrição	Quando aplicar	Responsável
<i>Brainstorming</i>	Identificação de Riscos	No início de cada projeto	Gestor de Risco
Entrevista Estruturada e Semiestruturada	Identificação de Riscos	No início de cada projeto	Gestor de Risco
Questionários	Avaliação de Riscos	No decorrer do projeto	Gestor de Risco
Plano de Ação	Tratamento de Riscos	No decorrer do projeto	Gestor de Risco
Relatório de Acompanhamento de Risco	Monitoramento e Controle de Riscos	No decorrer do projeto	Gestor de Risco
<i>Checklist</i>	Análise e Avaliação de Riscos e Tratamento de Riscos	No decorrer do projeto	Gestor de Risco

Fonte: Norma ISO 31010 (2019)

## 7. MONITORAMENTO E CONTROLE

Este documento será revisado semestralmente ou quando necessário. Todas as situações ou atividades não previstas neste documento deverão ser submetidas à Diretoria de TI que juntamente com sua equipe irão avaliá-las e aprová-las.

Imediatamente após sua aprovação, o Plano de Gestão de Riscos de Tecnologia da Informação e o Mapa de Gerenciamento de Riscos serão atualizados com o devido registro das alterações e encaminhados para o Comitê Gestor de TI.

Após a aprovação deste documento, os riscos apresentados pela área de TI serão registrados no *software* ForRisco, ferramenta adotada pelo IFTO para a gestão de riscos.

## 8. CRONOGRAMA

Este Plano será executado conforme as atividades apresentadas no Quadro 16.

Quadro 16 – Cronograma para execução do Plano de Gestão de Riscos de Tecnologia da Informação

Atividade	Início	Fim
Estabelecimento do Contexto	junho/2020	dezembro/2024
Identificação de Riscos	junho/2020	dezembro/2024
Análise de Riscos	junho/2020	dezembro/2024
Avaliação de Riscos	junho/2020	dezembro/2024
Tratamento de Riscos	junho/2020	dezembro/2024
Monitoramento e Análise Crítica	junho/2020	dezembro/2024
Comunicação e Consulta	junho/2020	dezembro/2024

Fonte: Diretoria de Tecnologia da Informação

## REFERÊNCIAS

BRASIL. Departamento de Segurança da Informação e Comunicações. **Instrução Normativa Complementar nº 4, de 15 de fevereiro de 2013. Gestão de Riscos de Segurança da Informação e Comunicações**. Brasília, DF: Presidência da República, 2013. Disponível em: [http://dsic.planalto.gov.br/legislacao/nc\\_04\\_grsic.pdf](http://dsic.planalto.gov.br/legislacao/nc_04_grsic.pdf). Acesso em: 10 maio 2020.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Controladoria-Geral da União. **Instrução Normativa Conjunta nº 1, de 10 de maio de 2016**. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. Brasília, DF: Presidência da República, 2016. Disponível em: [http://www.in.gov.br/materia/-/asset\\_publisher/Kujrw0TZC2Mb/content/id/21519355/do1-2016-05-11-instrucao-normativa-conjunta-n-1-de-10-de-maio-de-2016-21519197](http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/21519355/do1-2016-05-11-instrucao-normativa-conjunta-n-1-de-10-de-maio-de-2016-21519197). Acesso em: 10 maio 2020.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Secretaria de Tecnologia da Informação. **Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações do Sistema de Administração dos Recursos de Tecnologia da Informação do**

**Poder Executivo Federal.** Brasília, DF: Ministério do Planejamento, Desenvolvimento e Gestão, ago. 2016. Disponível em: <https://www.gov.br/governodigital/pt-br/sisp/mgr-sisp-v260816.pdf/view>. Acesso em: 10 maio 2020.

CONTROLADORIA-GERAL DA UNIÃO. **Metodologia de Gestão de Riscos.** Brasília, DF: Controladoria-Geral da União, abr. 2018. Disponível em: [https://repositorio.cgu.gov.br/bitstream/1/41833/5/Metodologia\\_gestao\\_riscos\\_2018.pdf](https://repositorio.cgu.gov.br/bitstream/1/41833/5/Metodologia_gestao_riscos_2018.pdf). Acesso em: 10 mai. 2020.

HM Government (HMG). **The Orange Book: Management of Risk Principles and Concepts.** 2020. Disponível em: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/866117/6.6266\\_HMT\\_Orange\\_Book\\_Update\\_v6\\_WEB.PDF](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866117/6.6266_HMT_Orange_Book_Update_v6_WEB.PDF). Acesso em: 11 jun. 2020.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TOCANTINS. **Gestão de riscos – IFTO:** metodologia de implantação. Palmas: IFTO, 2015. Disponível em: <http://www.ifto.edu.br/ifto/reitoria/diretoria-sistemica/infraestrutura/documentos-de-referencia/gestao-de-riscos-metodologia-do-ifto>. Acesso em: 10 jun. 2020.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **31000: 2018: Risk management:** guidelines, provides principles, framework and a process for managing risk. 2018.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **31010:2019: Risk Management:** Risk assessment techniques. 2019.

PROJECT MANAGEMENT INSTITUTE (PMI). **A Guide to the Project Management Body of Knowledge.** Project Management Institute. 5. ed. Pennsylvania, USA, 2013.

TRIBUNAL DE CONTAS DA UNIÃO. **Manual de Gestão de Riscos do TCU.** Brasília, DF: TCU, 2018a. Disponível em: <https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=FF8080816364D79801641D7B3C7B355A>. Acesso em: 10 jun. 2020.

TRIBUNAL DE CONTAS DA UNIÃO. **Referencial Básico de Gestão de Riscos.** SEGECEX/COGER. Brasília, DF: TCU, 2018b. Disponível em: [https://portal.tcu.gov.br/data/files/21/96/61/6E/05A1F6107AD96FE6F18818A8/Referencial\\_basico\\_gestao\\_riscos.pdf](https://portal.tcu.gov.br/data/files/21/96/61/6E/05A1F6107AD96FE6F18818A8/Referencial_basico_gestao_riscos.pdf). Acesso em: 10 jun. 2020.

TRIBUNAL DE CONTAS DA UNIÃO. **Gestão de riscos: avaliação da maturidade.** Brasília, DF: TCU, 2018c. Disponível em: [https://portal.tcu.gov.br/data/files/0F/A3/1D/0E/64A1F6107AD96FE6F18818A8/Gestao\\_riscos\\_avaliacao\\_maturidade.pdf](https://portal.tcu.gov.br/data/files/0F/A3/1D/0E/64A1F6107AD96FE6F18818A8/Gestao_riscos_avaliacao_maturidade.pdf). Acesso em: 10 jun. 2020.

ANTONIO DA LUZ JÚNIOR  
Reitor do Instituto Federal do Tocantins



Documento assinado eletronicamente por **Antonio da Luz Júnior, Reitor**, em 12/08/2020, às 18:30, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [http://sei.ifto.edu.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](http://sei.ifto.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **1011145** e o código CRC **6644B3A5**.

Avenida Joaquim Teotônio Segurado, Quadra 202 Sul, ACSU-SE 20, Conjunto 1, Lote 8 - Plano Diretor Sul — CEP 77020-450 Palmas/TO — (63) 3229-2200  
[portal.ifto.edu.br](http://portal.ifto.edu.br) — [reitoria@ifto.edu.br](mailto:reitoria@ifto.edu.br)