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

PROCESSO DE GESTÃO DE RISCOS EM TECNOLOGIA DA INFORMAÇÃO

1. INTRODUÇÃO

O processo de gestão de riscos de Tecnologia da informação do IFTO é responsável por identificar, avaliar, tratar, monitorar, controlar e documentar riscos relacionados com as seguintes áreas de TI: gestão de segurança da informação, desenvolvimento de soluções de TI, sistemas de informação, governança de TI e contratação de soluções de TI.

No IFTO, a gestão de riscos na área de TI é um conjunto de ações estratégicas que mapeiam e identificam possíveis ameaças a um determinado projeto, sistema, processo ou serviço. Este processo tem por objetivo evitar o desperdício de recursos públicos, bem como potencializar a efetividade de processos, garantindo que ações preventivas sejam feitas sempre que forem necessárias. Além disso, também permite criar uma estratégia para gerir os riscos envolvidos na falha de sistemas críticos ou de segurança da informação.

Neste sentido, a estrutura de gestão de riscos adotada pela área de Tecnologia da Informação (TI) do IFTO utiliza o modelo de gerenciamento de riscos proposto pela norma ISO 31000 (2018). Também leva em consideração 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). Utiliza a metodologia de gestão de riscos definida pelo IFTO (IFTO, 2015).

1.1. Objetivo

O processo de gestão de riscos de Tecnologia da Informação tem por objetivo geral definir o fluxo de atividades para identificar, avaliar, tratar, monitorar, controlar e documentar riscos de forma a tornar as ameaças em oportunidades de melhoria. Para isso, este processo tem os seguintes objetivos específicos:

a) Atenuar problemas, danos e prejuízos relativos à TI;

b) Prevenir ataques cibernéticos e roubos/violações de informações;

c) Definir métricas e indicadores para analisar continuamente os riscos em TI (de perda de dados, furto de informações, interrupção das atividades);

d) Incluir práticas contínuas de gestão de riscos;

e) Adaptar a infraestrutura de TI para acomodar os processos de gestão de risco em TI;

f) Definir papéis e responsabilidades dentro do processo.

1.2. Abrangência

Este processo abrange riscos relacionados com processos executados pela área de Tecnologia da Informação do IFTO, tais como: governança de TI, contratações de soluções de TI, desenvolvimento de soluções de TI, sistemas de informação, suporte operacional de TI e segurança da informação.

2. DEFINIÇÕES

Para melhor compreensão deste processo são apresentados termos, acrônimos e abreviações referente à temática gestão de riscos.

a) **Ameaça:** causa potencial de um incidente indesejado, que possui potencial para comprometer ativos através de exploração de vulnerabilidades.

b) **Ativos da informação:** 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.

c) **Consequência/impacto:** resultado de um evento que afeta os objetivos.

d) **Controle:** medida que mantém e/ou modifica o risco.

e) **Evento:** ocorrência ou mudança em um conjunto específico de circunstâncias.

f) **Gestão de riscos:** atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos.

g) **Incerteza:** estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade.

h) **Mapa de gerenciamento de riscos:** documento que relaciona os riscos identificados, sua origem, natureza e tipo.

i) **Matriz de riscos** (Matriz de Probabilidade x Impacto): documento que especifica combinações de probabilidade de ocorrência de um risco e do impacto causado por sua ocorrência, permitindo assim calcular o nível de risco a partir da multiplicação dos valores atribuídos à probabilidade e ao impacto.

j) **Plano de gestão de riscos:** plano que especifica a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos. Os componentes de gestão tipicamente incluem procedimentos, práticas, atribuição de responsabilidades, sequência e cronologia das atividades. O plano de gestão de riscos pode ser aplicado a um determinado produto, processo e projeto, em parte ou em toda a organização.

k) **Plano de tratamento de riscos:** plano que descreve as ações de tratamento do risco, identificando os responsáveis, com o objetivo de reduzir o risco a um nível aceitável (risco residual).

l) **Probabilidade:** chance de algo acontecer.

m) **Risco:** efeito da incerteza nos objetivos. Pode ser positivo, negativo ou ambos, e pode abordar, criar e resultar em oportunidades e ameaças.

n) **TI:** Tecnologia da Informação.

o) **Vulnerabilidade:** fraqueza de um determinado alvo ou controle que pode ser explorado por uma ameaça.

3. PROCESSO DE GESTÃO DE RISCOS DE TECNOLOGIA DA INFORMAÇÃO

O processo de gestão de riscos utilizado pela área de TI é composto por cinco atividades, conforme demonstra a figura 1. 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.

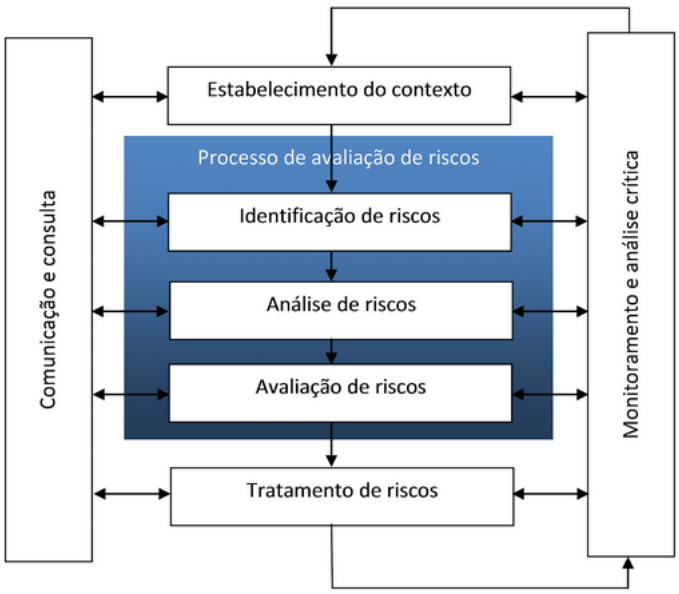

Figura 1 - Processo de gestão de riscos de TI (ISO 31000, 2018).

Conforme mostra a figura 1, o processo de gestão de riscos de TI utiliza como referência a norma ISO 31000 (2018) que é um modelo de referência sobre gestão de riscos. Este modelo está em conformidade com a legislação vigente. Este processo possui entrada, atividades e saídas que serão apresentadas na tabela 1.

Tabela 1 - Processo de gestão de riscos de TI

Objetivo	Gerenciar riscos relacionados com a área de TI que afetam a execução dos objetivos estratégicos do IFTO.
Entrada	Inventário de riscos de TI.
Atividades	1. Estabelecimento do contexto. 2. Avaliação de riscos (identificação, análise e avaliação de riscos). 3. Tratamento de riscos. 4. Comunicação e consulta. 5. Monitoramento e análise crítica.
Saída	Mapa de gerenciamento de riscos.
Ferramentas	- Planilha eletrônica. - Documentos eletrônicos.

Fonte: Diretoria de Tecnologia da Informação

Para gerenciar as atividades de gestão de riscos de TI apresentadas na tabela 1, a área de TI utiliza uma planilha eletrônica que documenta todas as tarefas realizadas. A partir desta planilha a gestão de riscos é feita através do software específico para gestão de riscos.

3.1. Entrada

Para iniciar o processo de gestão de riscos relacionados com a área de TI tem-se a lista de possíveis riscos associados com os processos de TI, são eles: Gestão de Segurança da Informação, Desenvolvimento de Soluções de TI, Governança de TI, Suporte Operacional de TI e Contratação de Soluções de TI. Neste processo este documento é denominado de inventário de riscos de TI.

3.2. Atividades

As atividades que compõem o processo de gestão de riscos de Tecnologia da Informação são: 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 irão detalhar estas atividades.

3.2.1. Estabelecimento do contexto

Na atividade de estabelecimento de contexto de riscos de TI é realizada análise da estrutura organizacional, responsabilidades, processos, sistemas de informação e relações com os demais setores da instituição. O contexto de riscos de TI no IFTO é dividido em contexto interno e externo.

a) **Contexto 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 contexto interno é a base para todos os outros componentes da estrutura de gestão de riscos, provendo disciplina e prontidão para a gestão de riscos. Envolve o entendimento dos objetivos e das estratégias que estão em vigor a fim de atingi–los; das capacidades da instituição em termos de recursos e conhecimento; dos fluxos de informação e processos de tomada de decisão; das partes interessadas internas; das percepções, valores e cultura; das políticas e processos; de normas e modelos de referência adotados pelo IFTO; das estruturas (por exemplo, governança, papéis e responsabilizações);

b) **Contexto externo:** avalia questões como o ambiente legal, social, cultural, político, financeiro, tecnológico, econômico, as relações com partes interessadas externas, sua percepção e seus valores. Envolve a familiarização com o ambiente em que a instituição opera, incluindo: os fatores culturais, políticos, legais, regulatórios, financeiros, econômicos e ambientais competitivos, seja em nível internacional, nacional, regional ou local; fatores–chave e tendências que tenham impacto sobre os objetivos da organização; percepções e valores das partes interessadas externas.

O estabelecimento do contexto da gestão de riscos de TI envolve a definição de responsabilidades; a definição da extensão das atividades de gestão de riscos a serem conduzidas, contemplando inclusões e exclusões específicas; a definição da extensão do projeto, processo, função ou atividade em termos de tempo e local; a definição das relações entre um projeto ou atividade específicos e outros projetos ou atividades da organização; a definição das metodologias do processo de avaliação de riscos; a definição dos critérios de risco; a definição de como o desempenho na gestão de riscos é avaliado; a identificação e a especificação das decisões e ações que precisam ser tomadas; identificação dos estudos necessários para escopo ou enquadramento, sua extensão e objetivos; os recursos requeridos para tais estudos.

3.2.2. Processo de avaliação de riscos

Este processo define quais os riscos identificados no processo de análise serão aceitos ou tratados, bem como priorizar o tratamento dos mesmos. A avaliação de riscos é composta pelas atividades: identificação, análise e avaliação de riscos que serão detalhadas nos próximos subitens.

3.2.2.1. Identificação de riscos

Esta atividade identifica os riscos e gera uma lista abrangente de eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos estratégicos. 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.

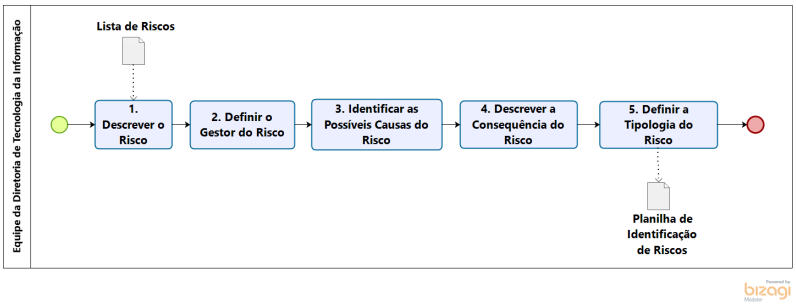

Figura 2 - Identificação de riscos

A figura 2 apresenta a atividade de 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 eletrônica 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 são 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 contribui para maior objetividade das análises quanto aos impactos. A tabela 2 apresenta a taxonomia de riscos utilizada para a identificação e análise de riscos.

Tabela 2 - Tipologia de riscos

Tipo/Categoria	Descrição
Operacionais	Eventos que podem comprometer as atividades da instituição, 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 da instituição.
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: Controladoria Geral da União (2016)

A tabela 2 descreve a tipologia de risco utilizada pela área de TI para a realização da atividade de identificação e análise de riscos. Os tipos de riscos também são divididos em categorias.

3.2.2.2. Análise de riscos

A atividade de análise de riscos refere-se ao desenvolvimento da compreensão sobre o risco e à determinação do nível de impacto. Ela 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 na análise de riscos.

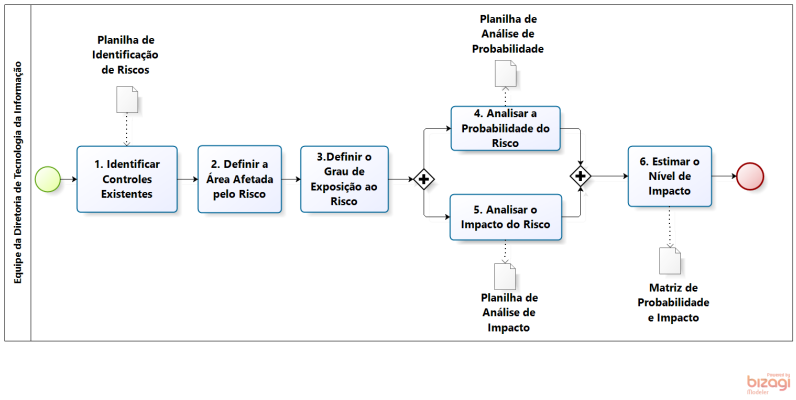

Figura 3 - Análise de riscos

Conforme demonstra a figura 3, a análise de riscos inicia-se com a tarefa de 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. O resultado desta atividade é registrado na matriz de probabilidade e 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 é feita a partir da definição de escalas de probabilidade e impacto através da técnica de matriz de probabilidade e impacto. 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. O 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. E o controle preventivo diz respeito a levantar quais ações podem ser realizadas visando à prevenção de possíveis causas de riscos (intencionais ou não). A tabela 3 apresenta os tipos de controle com o nível de maturidade e probabilidade de ocorrência do risco. Esta escala é uma adaptação do PMBOK publicada por PMI (2017).

Tabela 3 – 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: Diretoria de Tecnologia da Informação (adaptado de PMI, 2017)

A partir da definição do tipo de controle a ser aplicado a cada risco de acordo com a escala estabelecida na tabela 3, é feita a avaliação de forma a verificar o nível de controle a ser adotado. Para realizar esta atividade deve-se utilizar as recomendações contidas no manual de gestão de riscos divulgado pelo TCU em 2018 (TCU, 2018).

Para analisar riscos relacionados com a área de TI do IFTO utiliza-se 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 impacto.

A probabilidade consiste no resultado da materialização de um dado risco em determinado horizonte de tempo. É a chance do 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 de risco 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 é 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 a tabela 4. Esta escala é adaptada de TCU (2018b).

Tabela 4 - Escala de probabilidade de ocorrência do risco

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

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

A tabela 4 apresenta a escala de probabilidade do risco ocorrer, 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 é 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) é realizada uma média que define o nível de impacto. 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 é 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 agravar de acordo com o nível de tolerância (tempo) à ação saneadora.

A Diretoria de Tecnologia da Informação define uma escala adaptada do referencial básico de gestão de riscos do TCU (2018b) para realizar o cálculo do nível de impacto em razão de que o impacto varia de acordo com a área impactada. Quando um risco impactar mais de uma área, será considerada a área mais impactada.

Este 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. A tabela 5 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):

Tabela 5 - 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, de forma irreversível.	> 4.5

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

A tabela 5 define os pesos para cada impacto relacionado ao risco. Os pesos foram definidos de acordo com o nível de tolerância para o risco. A pontuação de impacto apresentada na tabela 6 leva em conta a escala definida pelo IFTO (2015).

Tabela 6 - 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 na tabela 6 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 é adotada a convenção apresentada na tabela 7.

Tabela 7 – Faixas de nível de risco

Faixa	Nível
Vermelha	muito alto (Transferir) - altíssima exposição.
Laranja	alto (Evitar) - alta exposição.
Amarela	médio (Mitigar) - média exposição.
Verde	baixo e muito baixo (Aceitar) - baixa exposição.

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

Os níveis de riscos identificados na tabela 7 são posicionados na matriz de riscos de acordo com a avaliação realizada de probabilidade de ocorrência e impacto. De acordo com o nível será definido o controle a ser adotado.

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 gerenciamento de riscos presente na planilha de identificação de riscos.

3.2.2.3. **Avaliação de riscos**

Esta atividade envolve a comparação do limite de exposição a riscos, a fim de determinar se o risco é aceitável ou não. A avaliação de riscos compara os 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.

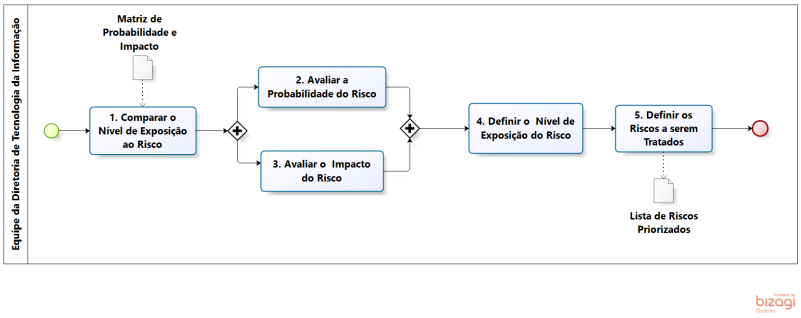

Figura 4 - Avaliação de riscos

Conforme mostra a 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. Ela é composta pelas tarefas comparar o nível de exposição ao risco, avaliar a probabilidade do risco, avaliar o impacto do risco, definir o nível de exposição do risco e definir 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 adotada pelo IFTO (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 Diretoria de Tecnologia da Informação. A matriz de riscos é uma adaptação de MPOG (2016), CGU (2018) E TCU (2018b).

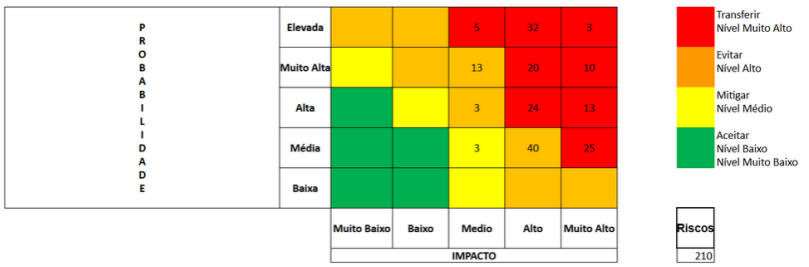

Figura 5 - Matriz de probabilidade e impacto (adaptado de MPOG (2016), CGU (2018) e TCU (2018b))

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. Nesta atividade são definidas atitudes perante os riscos a serem tratados de acordo com o nível de impacto para o processo.

A partir dos dados obtidos na matriz de probabilidade e impacto é construída a lista de riscos priorizados. Este artefato será utilizado pela atividade "tratamento de riscos".

3.2.3. Tratamento de riscos

O tratamento de riscos compreende o planejamento e a realização de ações para modificar o nível de risco. O nível de 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.

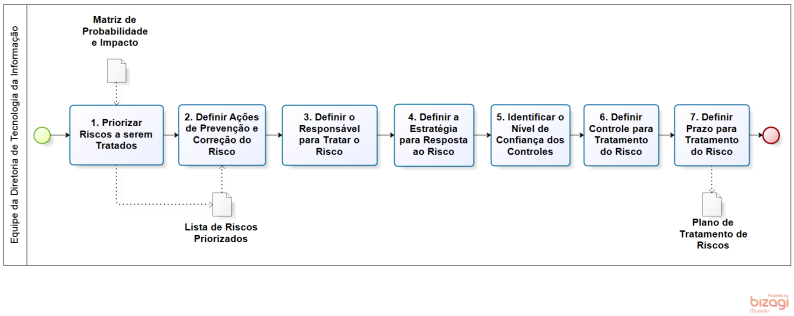

Figura 6 - Tratamento de riscos

De acordo com a figura 6, o tratamento de riscos se inicia com a tarefa de 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 estratégia para resposta ao risco, identifica o nível de confiança dos controles, o controle para tratamento do risco e o prazo para tratamento do risco. O resultado desta atividade é o plano de tratamento de riscos. Esta atividade envolve:

a) **Planejar as respostas aos 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, 2017).

b) **Estratégias para respostas aos riscos negativos ou ameaças:** para tratar os riscos negativos ou ameaças são utilizadas as estratégias: evitar ou eliminar, transferir, mitigar e aceitar, conforme mostra a tabela 8. Estas estratégias são adaptadas de CGU (2018).

Tabela 8 - 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 (Médio)	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: Controladoria Geral da União (2018)

A tabela 8 apresenta as estratégias utilizadas pela equipe da Diretoria de Tecnologia para mitigar os riscos negativos ou ameaças para a área de TI. A partir desta definição são definidos os controles a serem aplicados.

c) **Estratégias para respostas aos riscos positivos ou oportunidades:** para tratar os riscos positivos ou oportunidades deverão ser utilizadas as estratégias: explorar, compartilhar, melhorar e aceitar. A tabela 9 apresenta as estratégias definidas para a área de TI do IFTO.

Tabela 9 - 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 associada 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	A aceitação do risco envolve a criação de planos de contingências para serem implementados se os riscos ocorrerem.

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

A tabela 9 apresenta as estratégias utilizadas pela equipe da Diretoria de Tecnologia para mitigar os riscos positivos ou oportunidades para a área de TI. A partir desta definição são definidos os controles a serem aplicados.

d) **níveis de confiança dos controles:** deverão ser definidos os controles para a gestão de riscos de acordo com o nível de confiança existente. Recomenda-se o uso da escala definida pela Controladoria-Geral da União (CGU, 2018) e pelo Tribunal de Contas da União (TCU, 2018c). A Tabela 10 apresenta os níveis de confiança dos controles adotados pela área de TI no IFTO.

Tabela 10 - Níveis de confiança dos controles

Controle	Descrição
Inexistente	Nenhum nível de confiança. Controles inexistentes, mal desenhados ou mal implementados.
Fraco	Nível de confiança de 20%. Controles têm abordagens ad hoc, 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: Tribunal de Contas da União (2018c)

O artefato principal desta atividade é o plano de tratamento dos riscos. Este documento deve conter minimamente: descrição do risco, ação de tratamento, responsável, prazo e monitoramento.

3.2.4. Monitoramento e análise crítica

A atividade de 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. Esta atividade 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.

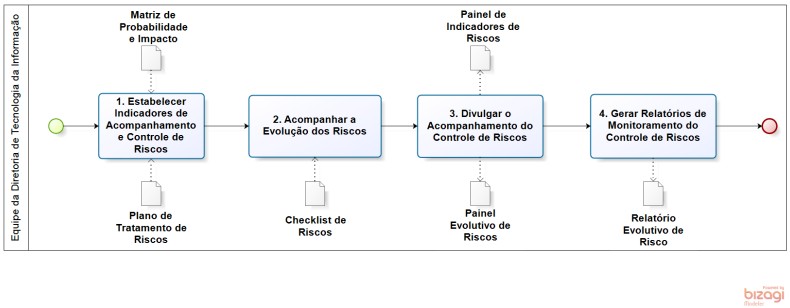

Figura 7 - Monitoramento e análise crítica

A atividade de monitoramento das ações de tratamento de riscos apresentada na figura 7 envolve 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. A atividade possui as seguintes tarefas: estabelecer indicadores de acompanhamento e controle de riscos, acompanhar a evolução dos riscos, divulgar o acompanhamento do controle de riscos e gerar relatórios de monitoramento do controle de riscos.

As tarefas de controle de riscos de TI são realizadas através de procedimentos estabelecidos e executados para mitigar os riscos definidos para o tratamento dos riscos. Estas tarefas são 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 é acompanhado sistematicamente em reuniões de planejamento de TI. Durante as reuniões são avaliadas as modificações dos atributos de situação, probabilidade de ocorrência e impacto dos riscos, bem como os valores para os gatilhos e a efetividade do plano de resposta para cada um dos riscos inventariados.

3.2.5. 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 processos 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.

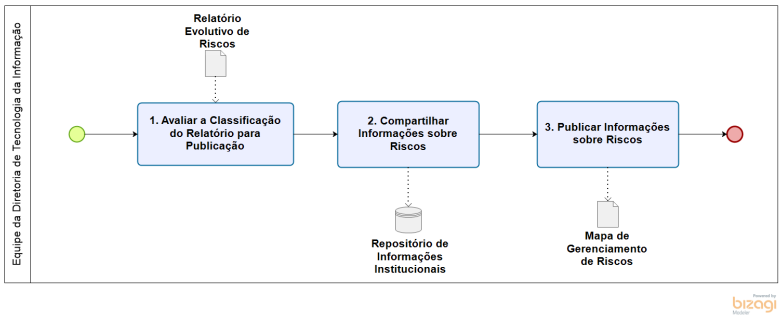

Figura 8 – Comunicação e consulta.

Conforme apresenta a figura 8, a comunicação e consulta é iniciada a partir da entrega do relatório evolutivo de riscos. Em seguida, é definida qual será a forma de publicação e compartilhamento da informação através do repositório digital de informações sobre riscos. O mapa de gerenciamento de riscos é compartilhado para que todas as coordenações de TI possam compreender os riscos inerentes ao setor de TI.

3.3. Saída

A saída do processo de gerenciamento de riscos de TI é o mapa de gerenciamento de riscos. A área de TI optou por utilizar uma planilha eletrônica como artefato de identificação centralizado de riscos. Para o monitoramento dos controles adotados será utilizado o software específico para gestão de riscos.

4. DOCUMENTOS DO PROCESSO

Vários são os documentos utilizados para padronização da gestão de riscos de TI. Todos os documentos estão concentrados em uma planilha eletrônica denominada de mapa de gerenciamento de riscos de TI. A área de TI concentra neste documento todos os riscos relacionados aos processos de TI: gestão de segurança da informação, desenvolvimento de soluções de TI, governança de TI, suporte operacional de TI e contratações de TI. A tabela 11 apresenta o mapeamento de gerenciamento de riscos de TI.

Tabela 11 - Mapeamento de gerenciamento de riscos de TI

Artefato	Descrição	Técnicas
Planilha de Identificação de Riscos	Identifica riscos relacionados à área de TI.	*Brainstorming*; entrevistas estruturadas ou semiestruturadas; *checklists.*
Planilha de Análise de Probabilidade	Calcula a probabilidade do 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 a resposta para o risco de acordo com a estratégia definida.	5W2H.

Fonte: Diretoria de Tecnologia da Informação (IFTO)

A tabela 11 detalha os artefatos que a área de TI utiliza para realizar a gestão de riscos de Tecnologia da Informação. Também apresenta as técnicas utilizadas para a identificação, análise, avaliação, tratamento, monitoramento e documentação de riscos.

5. PAPÉIS E RESPONSABILIDADES

Um papel é um conjunto de responsabilidades, atividades e autoridades definidas em um processo e atribuídas a uma pessoa, equipe ou função. Para realizar a gestão de riscos na área de TI são definidos papéis e responsabilidades para cada ator

envolvido no processo. Para cada risco mapeado e avaliado é associado um agente responsável formalmente identificado.

Na área de TI a Diretoria de TI é responsável pelo gerenciamento de todos os riscos mapeados na planilha "Mapa de Gerenciamento de Riscos". A tabela 12 detalha os papéis e responsabilidades de cada ator.

Tabela 12 - Responsabilidades e áreas de TI

Papel	Responsabilidades
Comitê Gestor de TI	- Aprovar o processo de gestão de riscos em Tecnologia da Informação. - Aprovar o plano de gestão de riscos em Tecnologia da Informação.
Comitê Gestor de Segurança da Informação	- Avaliar o plano de gestão de riscos de TI. - Elaborar o plano institucional de gestão de riscos, incluindo a definição do processo de gestão de riscos de segurança da informação.
Diretoria de Tecnologia da Informação (Dono do Processo)	- Definir as diretrizes de gestão de riscos específicas para os macroprocessos de TI (escopo, periodicidade/obrigatoriedade, critérios de risco, apetite de risco e designação dos papéis de gestão de riscos nos termos do processo em questão), em alinhamento com as diretrizes do Comitê Gestor de Riscos. - Definir quais processos de trabalho devem ser submetidos ao processo de gestão de riscos. - Revisar e aprovar o plano de tratamento de riscos.
Gestor de Riscos (Gerente do Processo)	- 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. - Elaborar e encaminhar o Plano de Tratamento de Riscos para o responsável pelo tratamento dos riscos. - Auxiliar o responsável pelo tratamento dos riscos na solução de impedimentos ou dificuldades na implementação das ações de tratamento de riscos, quando necessário. - Comunicar os riscos e o andamento das ações de tratamento às partes interessadas. - Monitorar o plano de tratamentos dos riscos.
Responsável pelo Tratamento de Riscos (Equipe de TI).	- Definir o contexto da análise de riscos, definindo os critérios da análise de riscos, a matriz de riscos (Probabilidade x Impacto) e os níveis de risco aceitáveis relevantes para o contexto em análise. - Associar um agente responsável para cada risco mapeado e avaliado, formalmente identificado para 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. - Implementar o plano de tratamento dos Riscos. - Informar o gestor de riscos qualquer dificuldade durante a implementação das ações de tratamento de riscos. - Informar o gestor de riscos sobre o surgimento de novos riscos a partir da implementação das ações de tratamento.

Fonte: Diretoria de Tecnologia da Informação

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. A tabela 13 apresenta as principais ferramentas usadas para gerenciar riscos na área de TI do IFTO.

Tabela 13 - Técnicas utilizadas para gestão de riscos de TI

Ferramenta	Descrição	Quando aplicar	Responsável
Brainstorming	Identificação de Riscos	No início de cada projeto	Gestor de Risco
Entrevista Estruturada e Semi Estruturada	Identificação de Riscos	No início de cada projeto	Gestor de Risco
Questionários	Avaliação de Riscos	No decorrer	Gestor de

		do projeto	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
Checklist	Análise e Avaliação de Riscos e Tratamento de Riscos	No decorrer do projeto	Gestor de Risco

Fonte: Norma ISO 31010 (2019)

Conforme demonstra a tabela 13 para cada atividade relacionada à gestão de riscos de TI podem ser utilizadas várias ferramentas recomendadas pela norma ISO 31010 (2019). A área de TI optou por utilizar as ferramentas apresentadas na tabela 13 tendo em vista serem as mais utilizadas pelas instituições públicas brasileiras.

7. MATRIZ RACI

A matriz RACI apresentada na tabela 14 é utilizada para definir com clareza as atribuições, papéis e responsabilidades de cada colaborador nas atividades do processo. A sigla RACI significa, em inglês: *Responsible, Accountable, Consulted e Informed.*

a) ***Responsible (Responsável):*** pessoa, função ou unidade organizacional responsável pela execução de uma atividade no âmbito de um processo;

b) ***Accountable (Responsabilizado):*** dono da atividade, deverá fornecer os meios para que a atividade possa ser executada, e será responsabilizado caso a atividade não alcance os seus objetivos; Cada atividade só pode possuir um Accountable;

c) ***Consulted (Consultado):*** pessoas que deverão ser consultadas durante a execução da atividade; As informações levantadas junto a essas pessoas tornam-se entradas para a execução da atividade;

d) ***Informed (Informado):*** pessoas que serão informadas acerca do progresso da execução da atividade.

Tabela 14 - Matriz de responsabilidade do processo

Atividade	Tarefa	DP	GP	ETI
Identificação de Riscos	Descrever o risco.	A	C/I	R
	Definir o gestor do risco.	A/R	C/I	I
	Identificar as possíveis causas do risco.	A	C/I	R
	Descrever a consequência do risco.	A	C/I	R
	Definir a Tipologia do risco.	A	C/I	R
Análise de Riscos	Identificar controles existentes.	A	C/I	R
	Definir a área afetada pelo risco.	A	C/I	R
	Definir o grau de exposição ao risco.	A	C/I	R
	Analisar a probabilidade do risco.	A/I	C/I	R
	Analisar o impacto do risco.	A/I	C/I	R
	Estimar o nível de impacto.	A/I	C/I	R
Avaliação de Riscos	Comparar o nível de exposição ao risco.	A/I	C/I	R
	Avaliar a probabilidade do risco.	A/I	C/I	R
	Avaliar o impacto do risco.	A/I	C/I	R
	Definir o nível de exposição do risco.	A/I	C/I	R
	Definir os riscos a serem tratados.	A/I	C/I	R
Tratamento de Riscos	Priorizar riscos a serem tratados.	A/I	C/I	R
	Definir ações de prevenção e correção do risco.	A/I	C/I	R
	Definir o responsável para tratar o risco.	A/I	R	C/I
	Definir a estratégia para resposta ao risco.	A/I	R	C/I
	Identificar o nível de confiança dos controles.	A/I	R	C/I
	Definir controle para tratamento do risco.	A/I	R	C/I
	Definir prazo para tratamento do risco.	A/I	R	C/I
Monitoramento e Análise Crítica	Estabelecer indicadores de acompanhamento e controle de riscos.	A/I	R	C/I
	Acompanhar a evolução dos riscos.	A/I	R	C/I
	Divulgar o acompanhamento do controle de riscos.	A/I	R	I
	Gerar relatórios de monitoramento do controle de riscos	A/I	R	C/I
Comunicação e Consulta	Avaliar a classificação do relatório para a publicação	A/I	R	C/I
	Compartilhar informações sobre riscos	A/I	R	C/I
	Publicar informações sobre riscos	A/I	R	C/I

Fonte: Diretoria de Tecnologia da Informação

Legenda:

DP: Dono do Processo (Diretoria de TI).

GP: Gerente do Processo (Coordenações de TI).

ETI: Equipe de Tecnologia da Informação.

8. INDICADOR DE DESEMPENHO

O processo de gestão de riscos será monitorado e constantemente medido através de indicadores de desempenho. Essas medidas serão consolidadas periodicamente pelo gerente do processo e farão parte do relatório gerencial do processo. Esse relatório tem como objetivo acompanhar a eficácia do processo, identificando tendências, falhas e oportunidades de correções, promovendo sempre a melhoria contínua. A tabela 15 apresenta o indicador de desempenho do processo.

Tabela 15 - Indicador de desempenho

Indicador	Quantidade de riscos gerenciados durante o ano.
Descrição	Quantificar riscos identificados e gerenciados durante o ano.
Objetivo	Calcular a quantidade de riscos gerenciados durante o ano.
Periodicidade	Anual.
Fórmula	Total de riscos gerenciados durante o ano.
Meta	Aumentar em 5% a quantidade de riscos de TI gerenciados durante o ano.
Fonte	ForRisco.

Fonte: Diretoria de Tecnologia da Informação

9. REFERÊNCIAS

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. (2016a). 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. 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. (2016b). 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. 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. 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/view. 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/planejamento-governanca-e-gestao/gestao-de-riscos/manual-de-gestao-de-riscos/. 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. 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. Acesso em: 10 jun. 2020.

Palmas, 08 de janeiro de 2021.

Kleyton Matos Moreira
Diretor de Tecnologia da Informação

Documento assinado eletronicamente por **Kleyton Matos Moreira**, **Diretor**, em 16/04/2021, às 09:42, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Paula Karini Dias Ferreira Amorim**, **Presidente**, em 16/04/2021, às 11:04, 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, informando o código verificador **1274411** e o código CRC **DDD4BA1F**.

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 — reitoria@ifto.edu.br

Referência: Processo nº 23235.000288/2021-05 SEI nº 1274411