Plano de Gestão de Riscos de TI

TRE-PI

SUMÁRIO

1. APRESENTAÇÃO

A Tecnologia da Informação é fundamental para o alcance dos objetivos estratégicos do TRE-PI, dessa forma, os riscos associados à área de TI devem ser gerenciados de forma eficaz. Este documento define o Plano de Gestão de Riscos de TI que deverá ser aplicado na Secretaria de Tecnologia da Informação.

De acordo com o TCU, em seu Referencial Básico de Gestão de Riscos, "*a sistematização da gestão de riscos em nível institucional aumenta a capacidade da organização para lidar com incertezas, estimula a transparência organizacional e contribui para o uso eficiente, eficaz e efetivo de recursos, bem como para o fortalecimento da reputação da instituição*".

Já o CNJ, na Resolução nº 370/2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), para o período 2021 a 2026, dispõe no Art. 37 que "*Cada órgão deverá elaborar Plano de Gestão de Riscos de TIC, com foco na continuidade de negócios, manutenção dos serviços e alinhado ao plano institucional de gestão de riscos, objetivando mitigar as ameaças mapeadas para atuar de forma preditiva e preventiva às possíveis incertezas*."

Nesse contexto, o presente plano contempla um conjunto de atividades que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos associados à Tecnologia da Informação, contribuindo para o fortalecimento da governança de TI, a tomada de decisões e o alcance dos objetivos institucionais.

2. OBJETIVO

Este documento visa direcionar as ações da Secretaria de Tecnologia da Informação, em cumprimento às diretrizes da Política de Gestão de Riscos de TI, estabelecidas na Resolução TRE-PI nº 354/2017, de forma a prever eventos ou situações que possam comprometer a execução dos objetivos estratégicos definidos no Plano Diretor de TI, reduzindo surpresas e prejuízos operacionais, otimizando o capital, fortalecendo as decisões em resposta aos riscos e aproveitando oportunidades, por meio de um processo de gestão de riscos de TI que permita a identificação, a análise, a avaliação, o tratamento, a priorização, o monitoramento e a comunicação dos riscos inerentes aos ativos de TI.

3. APLICABILIDADE

Este documento tem aplicabilidade para toda a Secretaria de Tecnologia da Informação do TRE-PI, e abrange as áreas de infraestrutura de TI, redes, segurança da informação, suporte técnico, manutenção de equipamentos de TI, desenvolvimento de sistemas, urnas eletrônicas, governança e gestão de TI.

4. ESCOPO

O escopo da Gestão de Riscos de TI é o de analisar os possíveis riscos relacionados aos ativos de TI que podem afetar os objetivos estratégicos da organização.

5. REFERÊNCIAS NORMATIVAS

Norma ABNT NBR ISO/73:2009
Norma ABNT NBR ISO/27.005:2011
Norma ABNT NBR ISO/31.000:2018
Norma ABNT NBR ISO/ 31.010:2019
Referencial Básico de Gestão de Riscos do TCU (2018)
Manual de Gestão de Riscos do TCU (2020)
Resolução CNJ nº 370/2021
Resolução TRE-PI nº 354/2017
Metodologia de Gestão de Riscos do TRE-PI

6. TERMOS E DEFINIÇÕES

Ameaça

Causa potencial de um incidente indesejado, que possui potencial para comprometer ativos através de exploração de vulnerabilidades.

Apetite a risco

É a quantidade e tipo de riscos que uma organização está preparada para buscar, reter ou assumir.

Ativos de TI

Qualquer elemento de valor para organização, seja tangível ou intangível, que esteja relacionado à Tecnologia da Informação.

Causa

Condição que viabiliza a concretização de um evento que afeta os objetivos estabelecidos, sendo resultante da junção das fontes de risco com as vulnerabilidades.

CDTI – Comitê Diretivo de Tecnologia da Informação

Responsável por orientar as ações e investimentos em Tecnologia da Informação, observando a estratégia institucional.

CGTI – Comitê Gestor de Tecnologia da Informação

Responsável pelos planos táticos e operacionais, análise de demandas, acompanhamento da execução de planos, estabelecimento de indicadores operacionais, dentre outros.

Consequências

Resultado de um evento que afeta os objetivos estabelecidos.

Critérios de risco

Termos de referência contra os quais a significância de um risco é avaliada, envolvendo a escala de probabilidade, a escala de impacto e a relação entre eles, bem como o apetite a risco estabelecido pelo Tribunal e, por fim, sua classificação.

Dimensões do Objetivo

Os objetivos são mensuráveis para que se tenha a dimensão dos possíveis prejuízos. Desta forma, as dimensões do objetivo classificam-se em Custo, Prazo (Cronograma), Escopo e Qualidade.

Escopo

É a soma total de todos os produtos do processo de trabalho e seus requisitos ou características.

Evento

Ocorrência ou mudança em um conjunto específico de circunstâncias.

Fonte de Risco

Elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco.

Impacto

Grandeza ou dimensão das consequências ou efeitos da ocorrência de um evento.

Órgãos de Controle Interno

Unidades administrativas, integrantes dos sistemas de controle interno da administração pública federal, incumbidas, entre outras funções, da verificação da consistência e qualidade dos controles internos, bem como do apoio às atividades de controle externo, exercidas pelo TCU.

Parte interessada (*Stakeholder*)

Pessoa ou organização que pode afetar, ser afetada ou perceber-se afetada por uma decisão ou atividade.

Probabilidade

Chance de algo acontecer.

Processo de Gestão de Riscos

Aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos.

Processo de Trabalho

Para as finalidades da Gestão de Riscos de TI do TRE-PI, processo de trabalho são os processos, projetos e ações relacionadas às competências e atribuições das unidades da Secretaria de Tecnologia da Informação do TRE-PI.

Risco

Possibilidade de algo acontecer e ter impacto negativo nos objetivos, sendo medido em termos de consequências e probabilidades.

Risco residual

Risco remanescente após o tratamento de risco ter sido implementado.

Vulnerabilidade

Propriedades intrínsecas de algo resultando em suscetibilidade a uma fonte de riscos que pode levar a um evento com uma consequência.

7. RESPONSABILIDADES

Compete ao CDTI:

- Promover a revisão periódica e a atualização da Política de Gestão de Riscos de TI (Resolução TRE-PI nº 354/2017);
- Assegurar a alocação dos recursos necessários à gestão de riscos de TI;
- Avaliar a adequação, a suficiência e a eficácia da estrutura de Gestão de Riscos de TI;
- Deliberar, após apreciação do CGTI, sobre os riscos considerados extremos e os riscos residuais considerados altos, que lhe forem submetidos por aquele Comitê Gestor;
- Assegurar que os riscos identificados pelo processo de gestão de riscos serão tratados por meio de ações a curto, médio ou longo prazos ou de aperfeiçoamento contínuo.

Compete ao CGTI:

- Revisar a Política de Gestão de Riscos de TI e apresentar proposta de atualização ao CDTI;
- Operacionalizar, no âmbito das unidades de TI, a aplicação dos recursos disponibilizados para a gestão de riscos de TI;
- Dirimir eventuais dúvidas dos proprietários de risco, na execução da Gestão de Riscos de TI;
- Deliberar sobre os riscos considerados médios e altos que, eventualmente, lhes forem apresentados pelos proprietários de risco;
- Submeter ao CDTI, após sua apreciação e manifestação, os riscos considerados extremos e os riscos residuais considerados altos;
- Subsidiar o CDTI com informações técnicas, visando auxiliá-lo no processo de tomada de decisão;
- Revisar continuamente a estrutura de Gestão de Riscos de TI, e submetê-la à aprovação do CDTI;
- Conscientizar os gestores sobre a importância da gestão de riscos de Tecnologia da Informação e a responsabilidade inerente a cada proprietário dos riscos;
- Escolher os processos de trabalho que devam ter os riscos gerenciados e tratados com prioridade em cada área técnica, à vista da dimensão dos prejuízos que possam causar.

Compete ao proprietário de risco, que no âmbito do TRE-PI é também o gestor de risco:

- Identificar, analisar, avaliar e gerir os riscos sob sua responsabilidade.
- Reportar ao CGTI os riscos que eventualmente extrapolarem sua competência e capacidade para gerenciamento;
- Encaminhar à unidade de assessoramento à governança de TI ou equivalente os Planos de Gestão de Riscos de TI de sua responsabilidade.
- Consultar e comunicar as partes interessadas no processo de gestão de riscos.

Compete à unidade de assessoramento à governança de TI ou equivalente:

- Proceder à consolidação dos planos de resposta aos riscos de TI a ela encaminhados, monitorando os riscos e reportando-os ao CGTI, periodicamente;

- Disseminar e dar suporte metodológico à implementação e à operacionalização do processo de gerenciamento de riscos nas unidades de TI, equipes e comissões;
- Propor ao CGTI melhorias para a presente Política de Gestão de Riscos de TI e para o modelo de processo correspondente.
- Revisar periodicamente a estrutura da gestão de riscos de TI, propondo ajustes quando necessário.

Compete à unidade de Controle Interno e Auditoria ou equivalente, no âmbito de suas atribuições:

- Incluir, nos planos de auditoria, ações de avaliação do gerenciamento de riscos de TI;
- Disponibilizar para a unidade de TI as ferramentas e técnicas utilizadas pela auditoria interna, para analisar riscos e controles administrativos na área de TI;
- Prover aconselhamento, facilitar grupos de discussão, orientar os proprietários de risco sobre riscos e controles administrativos, bem como promover o desenvolvimento de uma linguagem, estrutura e entendimento comuns;
- Avaliar os controles internos utilizados pela área de TI na gestão de seus riscos.

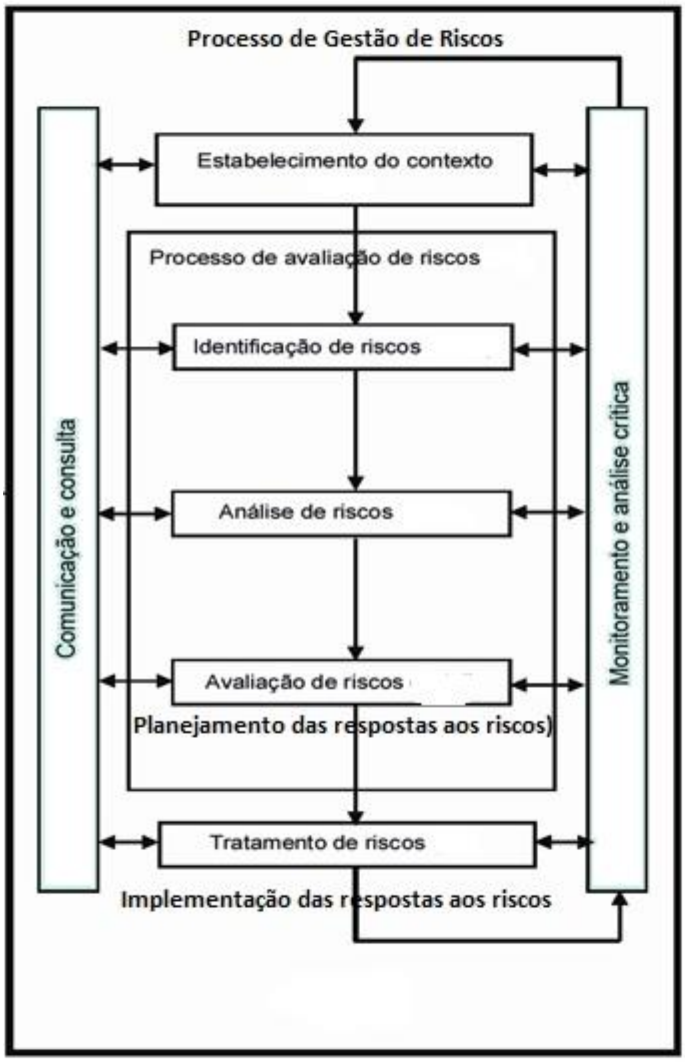
8. METODOLOGIA

A elaboração deste plano foi efetuada com base na Metodologia de Gerenciamento de Riscos do Tribunal Regional Eleitoral do Piauí, que é composta por processos que interagem de forma cíclica: Estabelecimento do Contexto, Identificação dos Riscos, Análise e Avaliação dos Riscos, Tratamento, Monitoramento e Comunicação dos Riscos.

9. PROCESSO DE GESTÃO DE RISCOS DE TI

O processo de gestão de riscos de TI ora adotado segue a estrutura disposta na Metodologia de Gestão de Riscos do Tribunal, e observa as definições do TCU, conforme detalhamento apresentado a seguir.

O processo de Gestão de Riscos é composto por um conjunto de etapas, cuja interdependência está demonstrada no diagrama abaixo, sendo consideradas as diretrizes estabelecidas pela ABNT NBR ISO 31000:2018:



9.1. Estabelecimento de Contexto

Esta etapa busca estabelecer os fatores internos e externos que, em conjunto com os critérios de riscos, formarão o ambiente de gerenciamento de riscos de TI. Devido à complexidade intrínseca à atividade de Estabelecimento do Contexto, recomenda-se o envolvimento de todas as partes interessadas, independentemente do nível hierárquico ou da área de atuação.

Outro fator determinante para a efetividade desta atividade é a abrangência do contexto a ser utilizado. Dessa forma, recomenda-se que seja considerado o maior número possível de elementos que contribuem, direta ou indiretamente, para potencializar o risco.

Cada proprietário de risco estabelecerá seu contexto específico, a fim de identificar os objetos de gestão de riscos mais relevantes para a unidade.

<u>**Análise do Contexto**</u>

Identificação: Descrever o objetivo estratégico, o processo de trabalho ou iniciativa corporativa.

Finalidade: Descrever os motivos (para quê?) do objetivo estratégico, o processo de trabalho ou a iniciativa corporativa foi estabelecido. Nessa descrição podem ser registrados os benefícios que serão gerados para a organização.

Principais entregas/resultados:

Para o caso de objetivo estratégico ou iniciativa corporativa:

Devem ser levados em consideração os principais resultados esperados ou entregas previstas, respectivamente.

Principais resultados esperados:

São os principais focos de atuação estabelecidos no Planejamento Estratégico Institucional (PEI) para os objetivos estratégicos. Para cada resultado são estabelecidas metas, mensuradas através de indicadores estratégicos, e/ou iniciativas, que auxiliarão no alcance da meta estabelecida. O mapeamento de riscos auxiliará na identificação de ações de controle e na identificação de processos de trabalho críticos para alcance dos resultados estabelecidos.

Principais entregas previstas:

São produtos/serviços gerados após a realização das atividades iniciativas corporativas. As entregas podem ser intermediárias, geradas em cada etapa da construção da iniciativa, cuja junção contribuirá para o alcance da entrega final.

Para o caso de processo de trabalho:

Para mapeamento de riscos de processos de trabalho devem ser levadas em consideração as principais atividades identificadas no fluxograma, responsáveis por gerar as entregas críticas (intermediárias), que contribuirão para o alcance do objetivo/entrega final do respectivo processo.

Fatores críticos de sucesso e status de implementação:

São fatores que, quando bem executados, definem e asseguram o alcance dos objetivos estratégicos, dos processos de trabalho e iniciativas corporativas. Em contrapartida, quando estes mesmos fatores são negligenciados ou ignorados, contribuem e muito para o fracasso os objetivos almejados.

Para análise de implantação, deve ser considerado o seguinte status:

- Implantado de forma Eficaz (IE) – Quando o fator crítico está implantado de forma eficaz na instituição, não havendo necessidade de melhorias;
- Implantado com Necessidade de Melhorias (INM) – Quando do fator crítica está implantado, mas há necessidade de melhorias imediatas;
- Em Fase de Implantação (FI) – Quando há plano ou ações em andamento para implantação do fator crítico;
- Não Implantado (NI): Quando não há plano ou ação em andamento para implantação do fator crítico.

<u>Análise de Cenário:</u>

Interno: São fatores internos da instituição, que podem impactar de forma positiva ou negativa os fatores críticos de sucesso.

Para efeito de análise de cenário interno, devem considerar os seguintes aspectos, mas não está limitado a:

- Normas, políticas e diretrizes organizacionais;
- Capacidades, entendidas em termo de recursos e conhecimentos;
- Identificar as pessoas envolvidas no processo e especialistas na área;
- Estrutura organizacional, funções e responsabilidades;

- Sistema de informações, fluxos de informações e processo de tomada de decisões;
- Cultura organizacional;
- Suporte tecnológico.

Externo: São fatores externos à instituição, que podem impactar de forma positiva ou negativa os fatores críticos de sucesso.

Para efeito de análise de cenário externo, deve-se considerar os seguintes aspectos, mas não está limitado a:

- Sociais, econômicos, políticos, tecnológicos, culturais e competitivos;
- Legais e regulamentares de órgãos externos;
- Relação com as partes interessadas e suas necessidades/expectativas.

9.2. Processo de Avaliação de Riscos

O processo de avaliação de riscos é composto por identificação, análise e avaliação de riscos (planejamento das respostas aos riscos).

9.2.1. 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.

A identificação dos riscos de TI será realizada inicialmente na etapa de mapeamento de processos e será revisada sempre que houver um redesenho do processo. Sendo um processo dinâmico (novos riscos podem surgir durante o acompanhamento do processo), significa que a lista de riscos de TI identificados poderá ser reavaliada. A frequência da revisão da lista é situacional e será definida pelo Gestor dos Riscos em acordo com o CGTI.

No processo de identificação dos riscos de TI deverá ser realizado o preenchimento dos dados de risco conforme o formulário de gestão de riscos de TI e nele serão descritos os itens: descrição do risco, identificação das possíveis causas do risco, descrição das consequências do risco.

Em consonância com as categorias de riscos definidas na Metodologia de Gerenciamento de Riscos do Tribunal, deverão ser utilizadas as seguintes categorias de riscos:

I. estratégicos: estão associados à tomada de decisão que pode afetar positivamente ou negativamente o alcance dos objetivos estratégicos do Tribunal, com a finalidade de alinhar e fornecer apoio à missão institucional;

II. operacionais: eventos normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;

III. imagem: eventos que podem comprometer a imagem da instituição junto à população ou a outros órgãos da Administração Pública;

VI. conformidade: estão associados ao cumprimento ou não cumprimento de princípios constitucionais, legislações ou regulamentações externas aplicáveis ao negócio, bem como de normas e procedimentos internos.

Para auxiliar a identificação de riscos, podem ser utilizadas técnicas e ferramentas como *brainstorming*, questionários, entrevistas, *checklist*, análise SWOT (forças, fraquezas, oportunidades e ameaças), análise de dados históricos, análise de premissas, opiniões especializadas, necessidades das partes interessadas e diagramas de causa e efeito.

A tabela a seguir apresenta exemplos de alguns dos principais riscos de Tecnologia da Informação:

RISCO	CAUSA	CONSEQUÊNCIA	CONTROLE
Falha Humana relacionada ao manuseio do grupo gerador de energia secundária.	Falha ao manusear equipamentos ou abastecimento do tanque de combustível.	Interrupção no fornecimento de energia secundária para o Data Center.	Capacitação de pessoal e realização de testes operacionais mensalmente.
Acesso físico não autorizado (indevido) a sala de equipamentos de rede e ao data Center.	Falhas dos controles de acesso físico aos racks de rede e ao Data Center.	Indisponibilidade de recursos, serviços e sistemas informatizados. Porta de acesso a roubo de informações.	Capacitação e controle de acesso físico aos equipamentos de rede e ao Data Center.
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 por curtos-circuitos, incêndios e/ou infiltrações.	Indisponibilidade de recursos, serviços e sistemas informatizados.	Adequado funcionamento do grupo gerador.
Falhas ou queima de componentes eletrônicos nos equipamentos de rede e do data Center.	Incidentes externos (surto elétrico ocasionado por problema na rede fornecedora de energia (tempestades) ou por incidentes internos em equipamentos energéticos (estabilizadores ou *no-breaks*).	Indisponibilidade de recursos, serviços e sistemas informatizados e até perda de dados.	Disponibilidade de equipamentos de proteção contra surtos elétricos e redundância de equipamentos energéticos do tipo estabilizador e *no-break*.
Indisponibilidade de *backups* de dados.	Cópia de segurança dos dados não disponíveis ou sem integridade em	Não recuperação de dados e perda total ou parcial de dados.	Disponibilidade de plano estratégico, tático e operacional de

	razão de indisponibilidade de rede, quedas ou oscilações de energia e/ou erros de configuração das estratégias de *backups*.		*backup* e restauração de dados.
Falhas na restauração de dados.	Erros de rede. Quedas ou oscilações de energia. Erros de configuração das estratégias de *backups*.	Não recuperação de dados. Perda de dados.	Estratégias de *backup* e restauração de dados.
Indisponibilidade de link principal de internet e de link de redundante.	Inexistência de contrato de prestação de serviços de internet para link backup com operadora distinta do link principal.	Indisponibilidade de recursos, serviços e sistemas informatizados.	Contrato de link redundante de internet com operadora diferente.
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 dos 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	Indisponibilidade de recursos, serviços e sistemas informatizados. Perda de dados.	Sistemas de Proteção contra raios, alagamentos e incêndios. Plano estratégico, tático e operacional para mitigar ou eliminar o risco.

	internos de escoamento de águas.		
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.	Disponibilidade de sistema de automação de ar-condicionado redundante.
Falhas no acesso ao *storage* de dados.	Indisponibilidade de rede de comunicação de dados. Oscilações de energia elétrica. Procedimento incorreto de acesso ao *storage*. Procedimento incorreto de configuração do *storage*.	Indisponibilidade de recursos, serviços e sistemas informatizados.	Disponibilidade de equipamentos redundantes. Grupo Gerador. Capacitação dos técnicos da área de TI.
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.	Indisponibilidade de recursos, serviços e sistemas informatizados.	Equipamentos Redundantes. Grupo Gerador. Capacitações.
Falhas na disponibilidade de rede lógica de dados na sede do TER-PI.	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.	Indisponibilidade de recursos, serviços e sistemas informatizados.	Equipamentos redundantes. Grupo Gerador. Capacitações.

	Ausência de capacitações em redes de comunicação de dados.		
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.

9.2.2. Análise e Avaliação dos Riscos

A etapa de análise e avaliação dos riscos consiste em realizar a análise qualitativa dos riscos, que definirá as possíveis respostas às ocorrências em conformidade com o nível de criticidade definido. É também nesta etapa que se identificará os riscos críticos.

A análise e avaliação dos riscos de TI serão realizadas em duas etapas: a análise de riscos inerentes e a análise de risco residual. A análise de riscos fornece subsídios para a avaliação de riscos, bem como para as estratégias, métodos e decisões de tratamento dos riscos.

Essa fase envolve a apreciação das causas e das fontes de riscos, suas consequências negativas, e a probabilidade de que essas consequências venham a ocorrer. Devem ser identificados os fatores que afetam as consequências e a probabilidade de ocorrência dos riscos, ou a combinação de ambos, confrontados com os controles existentes, a fim de testar a eficácia e a eficiência desses controles.

A combinação das consequências, as quais podem ser expressas em termos de impactos tangíveis e intangíveis, com a probabilidade serve para determinar o nível e tipo do risco.

Por conta da interdependência dos diversos riscos e das suas fontes, a análise de riscos poderá ser realizada em diferentes níveis de detalhe, dependendo do risco, da finalidade da análise, das informações, dos dados e dos recursos disponíveis.

A avaliação de riscos utiliza os resultados da análise de riscos como subsídio para a tomada de decisões sobre quais riscos necessitam ser tratados e quais terão prioridade no tratamento. A avaliação deve considerar a probabilidade de ocorrência, bem como o impacto sobre os objetivos. Quanto maior a probabilidade e o impacto, maior será o nível do risco.

Análise de riscos inerentes

Definimos como riscos inerentes (puros), aqueles avaliados sem a consideração das medidas de controle (caso existam), e os residuais, aqueles avaliados, considerando as medidas de controle.

A análise de riscos inerente é realizada a partir de entrevistas com os executores dos processos de trabalho ou a partir de reuniões com todos os envolvidos. Todos os envolvidos diretamente ou indiretamente na realização das atividades, que fazem parte do processo avaliado, são convocados a participar e a classificar os eventos (riscos) quanto a sua probabilidade e impacto. O passo seguinte é a multiplicação da probabilidade pelo impacto gerando assim o nível de criticidade de cada risco.

Para essa atividade, serão consideradas as escalas de probabilidade e impacto indicadas a seguir.

Tabela - Escala de probabilidade dos riscos

Aspectos Avaliados	**Evento pode ocorrer apenas de maneira excepcional**	**Evento pode ocorrer em algum momento**	**Evento deve ocorrer em algum momento**	**Evento que provavelmente ocorra na maioria das circunstâncias**	**Evento esperado que ocorra na maioria das circunstâncias**
Frequência	Muito baixa (< 21%)	Baixa (>=21%= 40%)	Média (>=30% =50%)	Alta (>=41%<= 80%)	Muito alta (>80%)
Peso	**1**	**2**	**3**	**4**	**5**

Para que o nível de impacto seja definido, é necessário considerar quais são as dimensões (custo, prazo, escopo e qualidade) do objetivo do processo de trabalho avaliado que serão influenciadas direta ou indiretamente. O impacto está associado às consequências do evento ocorrido.

CUSTO (aumento %)	PRAZO (atraso %)	ESCOPO (afetação)	QUALIDADE (degradação)	NÍVEL
Até 5	Até 5	Insignificante	Irrisória	1
> 5 Até 10	> 5 Até 10	Pouco	Pouco	2
> 10 Até 15	> 10 Até 15	Significativa	Relevante	3
> 15 Até 20	> 15 Até 20	Muito significativa	Muito relevante	4
> 20	>20	Ampla	Grave	5

Impacto nas Dimensões do Objetivo

Vale salientar que nem sempre o nível será o mesmo para todas as dimensões. Caso isso aconteça, considerar-se-á o nível mais alto.

Ao final da avaliação qualitativa inerente, o gestor de riscos, deverá priorizar os riscos das atividades dos processos de trabalho a partir do cruzamento das escalas de probabilidade e impacto supracitadas, conforme o quadro abaixo.

	Probabilidade	Muito baixa 1	Baixa 2	Média 3	Alta 4	Muito alta 5
Impacto	5 – Extremo	5	10	15	20	25
	4 – Alto	4	8	12	16	20
	3 – Moderado	3	6	9	12	15
	2 – Baixo	2	4	6	8	10
	1 – Irrelevante	1	2	3	4	5

Escala de Criticidade do Risco

Risco Baixo	1 - 4
Risco Moderado	5 - 9
Risco Alto	10 - 16
Risco Crítico	17 - 25

A criticidade dos riscos (eventos), definida pelo cruzamento da probabilidade e impacto, será identificada por cores que traduzirão a severidade e de forma consequente as medidas a serem tomadas. No quadro seguinte identificam-se os níveis de riscos desta metodologia e o apetite a riscos de TI do Tribunal.

O apetite a risco está relacionado à quantidade de risco de TI que o Tribunal se dispõe a aceitar na busca por agregar valor aos serviços prestados para a sociedade. Não cabe aos proprietários de riscos fazer adequações neste critério de riscos.

NÍVEL DE RISCO	DESCRIÇÃO DO NÍVEL DE RISCO
Risco Crítico/extremo	Indica um nível de risco absolutamente inaceitável, muito além do apetite a risco da organização.
Risco Alto	Indica que o risco inerente será reduzido a um nível compatível com a tolerância a riscos (indica um nível de risco inaceitável, além do apetite a risco definido para o TRE-PI).
Risco Moderado	Indica que o risco inerente será reduzido a um nível compatível com a tolerância a riscos (indica um nível de risco aceitável, dentro do apetite risco definido para o TRE-PI).
Risco Baixo	Indica que o risco inerente já está dentro da tolerância a risco.

Ao final, com a definição do nível de risco, será possível estabelecer a ordem de priorização dos riscos. Neste sentido, os riscos críticos, ou de cor vermelha, podem ser imediatamente tratados, quanto à identificação de possíveis respostas, em caso de ocorrência.

Análise de riscos residuais

A análise dos riscos residuais é realizada logo após o término da avaliação anterior. Nesta etapa da análise e avaliação dos riscos, se busca tratar os riscos inerentes, considerando as medidas de controle (caso existam) correspondentes a cada evento. Para cada evento, devem ser identificados os controles existentes, conforme abaixo.

- Descrição do Controle Atual

Deverá ser descrito, livremente, os atuais controles de riscos analisados pela Unidade.

- Avaliação quanto ao Desenho do Controle

(1) Não há sistema de Controle;
(2) Há procedimento de controle para algumas atividades, porém informais;
(3) Controles não foram planejados formalmente, mas são executados de acordo com a experiência dos servidores;
(4) É desenhado um sistema de controle integrado adequadamente planejado, discutido e documentado. O sistema de controle vigente é eficaz, mas não prevê revisões periódicas;
(5) O sistema de controle é eficaz na gestão de riscos (adequadamente planejado, discutido, testado e documentado com correções ou aperfeiçoamentos planejados de forma tempestiva).

- Avaliação quanto a Operação do Controle

(1) Não há Sistema de Controle
(2) Controle parcialmente executado e com deficiências;
(3) Controle parcialmente executado;
(4) Controle implantado e executado de maneira periódica e quase sempre uniforme. Avaliação dos controles é feita com alguma periodicidade;
(5) Controle implantado e executado de maneira uniforme pela equipe e na frequência desejada. Periodicamente os controles são testados e aperfeiçoados.

Ao final é realizada nova avaliação qualitativa a partir da probabilidade de ocorrência e do impacto das atividades, considerando a mesma escala de probabilidade e impacto. O passo seguinte é a multiplicação da probabilidade pelo impacto, gerando assim o nível de criticidade de cada risco após as medidas de controle.

A expectativa é que avaliação de risco inerente seja diferente da avaliação de risco residual, já que neste último se consideram os controles existentes.

Em caso de riscos extremos e/ou residuais altos, o CGTI deverá reportá-los ao CDTI, após avaliação técnica, incluindo propostas de ações a serem adotadas.

9.3. Tratamento dos riscos

O tratamento dos riscos é a definição da estratégia ou mescla de estratégias que deverão definir resposta aos riscos negativos avaliados qualitativamente na etapa de análise e avalição do risco.

A finalidade desta etapa é determinar os tipos de estratégias que devem ser utilizados para tratar os riscos avaliados na etapa anterior, estabelecendo ações para tratamento e composição do Plano de Gestão de Riscos de TI.

Tipos de estratégias

- Risco Positivo (Oportunidade): explorar, compartilhar, melhorar e aceitar;
- Risco Negativo (Ameaça): prevenir, eliminar, transferir, mitigar e aceitar.

Os Riscos Positivos na metodologia do TRE-PI serão suprimidos. Para os riscos negativos serão adotadas as seguintes estratégias:

- Evitar: É uma estratégia de resposta ao risco em que se age para eliminar totalmente a ameaça;
- Reduzir/mitigar: É uma estratégia de resposta ao risco em que se age para reduzir a probabilidade de ocorrência, ou o impacto do risco.
- Transferir: É uma estratégia de resposta ao risco em que se age para transferir o impacto de uma ameaça para terceiros.
- Aceitar Riscos: É uma estratégia de resposta ao risco em que se decide reconhecer a existência do risco e não agir, a menos que o risco ocorra.

A aceitação do risco é considerada quando o nível de risco é muito baixo ou ainda quando o custo-benefício para a implementação da resposta ao risco não se traduz em vantagem.

Quadro do nível de risco e ações de controle

Nível de Risco	Tipo de Resposta	Ação de Controle
Risco Crítico	**Evitar**	Promover ações que evitem/eliminem as causas e/ou efeitos
Risco Alto	**Reduzir**	Promover ações para reduzir a probabilidade ou impacto dos riscos, ou ambos
Risco Moderado	**Compartilhar ou Transferir**	Reduzir a probabilidade ou impacto pela transferência ou compartilhamento de uma parte do risco. (Exemplo: contratação de seguro ou terceirização da atividade).
Risco Baixo	**Aceitar**	Conviver com o evento de risco mantendo práticas e procedimentos existentes

Após a definição da resposta ao risco, será necessário detalhamento da medida a ser tomada e o responsável pelo seu acionamento.

Ações para tratamento dos riscos de TI

De acordo com a criticidade dos riscos haverá necessidade de viabilizar resposta ao risco através da elaboração de plano de ação a ser aplicado ao risco analisado. No formulário de gestão de riscos de TI serão contemplados os campos de preenchimento obrigatório.

Tipos de ação para o tratamento dos riscos de TI:

Para as ameaças serão adotadas ações corretivas de intervenção (risco crítico, alto e moderado) ou ação de controle interno.

- Ação de intervenção ou corretiva: ação corretiva é ação destinada a prevenir a repetição da situação, devendo levar em consideração a causa originária do problema.
- Ação de Controle ou controle interno: são procedimentos, regras ou práticas rotineiras com a finalidade de controlar o risco negativo ou positivo. Exemplos: Instruções Normativas aprovadas e disseminadas, acompanhamento periódico de execução de ações por parte dos Comitês Setoriais, realização de reuniões periódicas de acompanhamento, divulgação sistemática de resultados, etc.

Mesmo após o tratamento de determinado risco, pode haver risco residual. Para que o risco residual seja aceito, é imprescindível considerar o apetite a risco de TI que o TRE-PI está disposto a se expor na busca de seus objetivos.

9.4. Monitoramento e Análise Crítica do Risco

A fase de monitoramento e análise crítica é etapa essencial da gestão de riscos de TI e tem por finalidade:

- Garantir que os controles sejam eficazes e eficientes no projeto e na operação, de forma que as ações de respostas ao risco tenham o resultado esperado ou se novas respostas devem ser desenvolvidas;
- Obter informações adicionais para melhorar a avaliação dos riscos.
- Analisar os eventos, as mudanças, e aprender com o sucesso ou fracasso do tratamento do risco.
- Detectar mudanças nos contextos externo e interno, incluindo alterações nos critérios de risco e no próprio risco, as quais podem exigir a revisão da forma de tratar os riscos e das prioridades.
- Identificar os riscos emergentes, que poderão surgir após o processo de análise crítica, reiniciando o ciclo do processo de gestão de riscos.
- Identificar os riscos que deixaram de existir.
- Mensurar o resultado de indicadores operacionais da gestão de riscos de TI.

O presente plano sugere que seja utilizado o indicador de resultado KR 7.1, definido no PDTI, ciclo 2021-2026, para o processo de gestão de riscos de TI do TRE-PI:

KR 7.1 – Implementar a gestão de riscos em 100% dos serviços críticos até 2022

9.5. Comunicação e consulta

A comunicação e a consulta têm como objetivo facilitar a troca de informações, levando em consideração os aspectos de confidencialidade, integridade e confiabilidade.

A comunicação e a consulta às partes interessadas acontecem durante todas as fases do processo de gestão de riscos, devendo ser cíclica e executada sempre que necessário, tendo como objetivo a melhoria contínua.

10. CONCLUSÃO

Em conformidade com as normas NBR ISO 31000:2018 e NBR ISO 27005:2011, este Plano de Gestão de Riscos de TI mostrou que gerenciar riscos de TI com eficiência é um desafio, porém é também um fator crítico de sucesso na execução dos processos de trabalho da organização.

Além disso, o uso de um processo adequado pode permitir o melhor tratamento dos riscos identificados e ganho de qualidade, desta forma, os proprietários do risco poderão aumentar a efetividade da gestão, alcançando melhores resultados.

O processo de gestão de riscos de TI definido por este plano contempla as atividades de estabelecimento do contexto, identificação de riscos, análise de riscos, avaliação de riscos, tratamento de riscos, monitoramento e análise crítica, e comunicação e consulta. Adicionalmente, fornece formulários que contemplam cada uma dessas atividades.

Com a revisão do processo em 2022, busca-se facilitar a gestão dos riscos de TI por meio da unificação dos formulários de análise do contexto, identificação de riscos, análise e avaliação de riscos, tratamento de riscos, monitoramento e análise crítica em um único modelo, simplificando sobremaneira o seu preenchimento.

ANEXOS

Formulários e Indicador

TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ
Secretaria de Tecnologia da Informação

FORMULÁRIO DE GESTÃO DE RISCOS DE TI

IDENTIFICAÇÃO DO ESCOPO			
Ativo / Processo / Projeto:	**Objetivo do Ativo / Processo / Projeto:**		
Responsável pela avaliação / Unidade:	**Data da avaliação:**	**Responsável pela revisão / Unidade:**	**Data da revisão:**

GESTÃO DE RISCOS DE TI																				
Identificação dos riscos							**Análise dos riscos**			**Avaliação do risco inerente**			**Ações de tratamento**					**Monitoramento**		
ID	**Descrição do risco**	**Contexto**	**Causa**	**Evento**	**Consequência**	**Categoria**	**Probabilidade**	**Impacto**	**Nível**	**Controle existente**	**Eficácia**	**Risco residual**	**Resposta ao risco**	**Descrição**	**Responsável**	**Data início**	**Data fim**	**Periodicidade**	**Status**	**Observação**
R.1	Descreva o risco	Interno ou externo				Estratégico Operacional Imagem Conformidade	1 - Muito baixa 2- Baixa 3- Média 4- Alta 5- Muito alta	1 - Irrelevante 2- Baixo 3- Médio 4- Alto 5- Muito alto	Baixo Moderado Alto Crítico	Descreva o controle	Inexistente Fraco Mediano Satisfatório Forte		Evitar Reduzir Compartilhar ou Transferir Aceitar						Não iniciado Em andamento Concluído Cancelado	
R.2																				
R.3																				
R.4																				
R.5																				
R.6																				
R.7																				
R.8																				
R.9																				
R.10																				
R.11																				
R.12																				
R.13																				
R.14																				
R.15																				

FORMULÁRIO PARA COMUNICAÇÃO DE RISCOS DE TI

IDENTIFICAÇÃO DO ESCOPO						
Ativo / Processo /Projeto:			Objetivo do Ativo / Processo / Projeto:			
COMUNICAÇÃO DE RISCOS DE TI						
ID	DESCRIÇÃO DO RISCO	COMUNICADOR	PROPÓSITO	MÉTODO DE COMUNICAÇÃO	DATA DA COMUNICAÇÃO	FREQUÊNCIA
			Informar Consultar	E-mail Memorando Ofício Intranet Treinamento Reunião		Ad hoc Esporádica Semanal Mensal Trimestral Semestral Anual
			Informar Consultar	E-mail Memorando Ofício Intranet Treinamento Reunião		Ad hoc Esporádica Semanal Mensal Trimestral Semestral Anual

INDICADOR DE RESULTADO

OBJETIVO ESTRATÉGICO	RESULTADO-CHAVE		FÓRMULA	UNIDADE PARA CUMPRIMENTO	UNIDADE PARA MEDIÇÃO	VALOR ATUAL	METAS					
							2021	2022	2023	2024	2025	2026
Aprimorar a Segurança da Informação e Proteção de Dados	KR 7.1	Implementar a gestão de riscos em 100% dos serviços críticos até 2022	Quantidade de serviços críticos com gestão de riscos implementada pelo total de serviços críticos	CODIN	CODIN	0%	70%	100%	100%	100%	100%	100%