SUMÁRIO

1. INTRODUÇÃO

A sistemática da gestão de riscos constitui uma estratégia que aumenta a capacidade da DTI do TCE-AL para lidar com incertezas, estimula a transparência, contribui para o uso eficiente de recursos e melhora a entrega de serviços de TI ao público interno e à sociedade.

Neste contexto, a referida política visa orientar e direcionar as atividades a serem conduzidas na DTI do TCE-AL, de forma a prever eventos ou situações que possam comprometer a execução dos objetivos definidos no **Plano Diretor de Tecnologia da Informação PDTI (2024-2026)**. Com isso, espera-se aumentar a probabilidade e impacto de eventos positivos, reduzir os negativos e direcionar a equipe de TI sobre como os riscos deverão ser gerenciados e tratados.

2. OBJETIVO

A Gestão de Riscos em Tecnologia da Informação na DTI do TCE-AL tem a finalidade 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. Esta política fornece uma abordagem para a gestão de riscos relacionados a TI por meio de um conjunto de atividades e tarefas que permitem o estabelecimento do contexto, a identificação, avaliação, priorização, tratamento, comunicação e implementação de medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação na DTI do TCE-AL, a partir do uso eficiente e eficaz dos recursos, promovendo a entrega de valor baseado nos seguintes objetivos:

a) Definir atividades e tarefas que compõem o processo de gestão de riscos;

b) Encorajar uma gestão proativa dos riscos;

c) Identificar e tratar riscos com envolvimento das equipes e patrocínio da Direção na DTI;

d) Melhorar a identificação de oportunidades e ameaças;

e) Melhorar a governança e gestão em TI dentro das práticas definidas na **Política de Governança de TI** definindo papéis e responsabilidades de cada envolvido no processo de gestão de riscos;

3. RESPONSABILIDADES E AUTORIDADES

Diretoria de TI: responsável por identificar, analisar, propor soluções, acompanhar o tratamento dos riscos e avaliar os resultados obtidos.

Gestor de Governança e Segurança da Informação: responsáveis pela avaliação das propostas de tratamento dos riscos identificados, atestando a validade, momento e modo de implementação de cada tratamento.

Responsáveis pelo tratamento dos riscos: colaboradores designados pela DTI do TCE-AL com aptidão para implantar as ações de tratamento dos riscos.

4. ABRANGÊNCIA

A política em tela permeia todo o ciclo de vida das iniciativas para desenvolvimento, implementação e gestão de soluções e serviços gerenciadas pela DTI do TCE-AL. Abrange as equipes de governança e gestão de TI, infraestrutura de TI, desenvolvimento e sustentação de sistemas, manutenção em equipamentos de TI, gestão em banco de dados, processos e projetos, serviços de TI, suporte operacional e segurança da informação trabalhando em sintonia para identificação e implementação de medidas protetivas necessárias para minimizar ou eliminar os riscos nos seguintes pilares:

a) Riscos Estratégicos: riscos identificados e analisados no escopo da elaboração dos artefatos, nos sistemas e serviços estratégicos da DTI.

b) Riscos de Segurança: riscos identificados e analisados no escopo de segurança da informação e comunicação ou normas relacionadas, considerando-se principalmente os sistemas e serviços críticos da DTI.

c) Riscos em Contratações: riscos identificados, avaliados, tratados e monitorados no âmbito de cada contratação, desde a fase de planejamento até a fase de execução, incluindo a vigência contratual da solução ou serviço implantado.

d) Riscos em Projetos: riscos gerenciados no âmbito de cada projeto devendo ser identificados pelos gestores deles.

e) Riscos em Processos: identificados nos processos mapeados e/ou instituídos em toda DTI.

f) Riscos Tecnológicos: possibilidade de ocorrência de falhas em sistemas de tecnologia da informação com impactos nos objetivos ou na execução de processos da DTI.

5. REFERÊNCIAS

Manual de Classificação e Tratamento de Informações Sigilosas;

Manual de Gerenciamento de Permissões de Acesso;

Norma ABNT ISO/IEC 20000:2018 para Gerenciamento de Serviços de TI;

Norma ABNT ISO/IEC 27001:2022 para Gestão da Segurança da Informação, Segurança Cibernética e Proteção à Privacidade;

ABNT NBR ISO 27005:2023 para Gestão de Riscos de Segurança da Informação;

Norma ABNT ISO/IEC 29134:2017 - Tecnologia da Informação - Técnicas de Segurança, Avaliação de Impacto de Privacidade;

Norma ABNT NBR ISO/IEC 27005:2023 - Gestão de Riscos de TI;

Norma ABNT NBR ISO 31000:2018 - Diretrizes para Gestão de Riscos;

Plano de Aquisições e Contratações de TI na DTI do TCE-AL;

Plano Diretor de Tecnologia da Informação PDTI (2024-2026);

Política Corporativa de Segurança da Informação do TCE-AL;

Política de Controle de Acesso Lógico e Físico do TCE-AL;

Política de Gestão de Backup e Recuperação de Dados;

Política de Gestão de Fornecedores do TCE-AL;

Política de Gestão de Riscos de TI;

Política de Governança de TI;

Política de Privacidade e Proteção de Dados Pessoais do TCE-AL;

Política de Tecnologia da Informação do TCE-AL;

Processo de Gestão e Análise de Vulnerabilidades de TI;

Procedimento Operacional de Gestão de Incidentes e Requisições;

Procedimento Operacional de Gestão de Mudanças.

6. CONCEITOS E DEFINIÇÕES

Ameaça: causa potencial de um incidente indesejado que pode comprometer ativos através da exploração de vulnerabilidades;

Ativos da Informação: meios de armazenamento, transmissão e processamento, sistemas de informação, bem como, locais onde se encontram esses meios e as pessoas que a eles têm acesso;

Controle: medida que mantém e/ou modifica o risco;

Evento: ocorrência ou mudança em um conjunto específico de circunstâncias;

Gestão de Riscos: processo que contempla atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização dos seus objetivos;

Impacto: consequências para a organização caso um risco venha acontecer de fato. Sendo negativo incorre em perdas financeiras, de clientes e danos ao ambiente operacional. Sendo positivo representa novas oportunidades de negócios;

Partes Interessadas: pessoa ou organização que pode afetar, ser afetada ou perceber-se afetada por uma decisão ou atividade;

Plano Diretor de Tecnologia da Informação (PDTI): instrumento de diagnóstico, planejamento e gestão dos recursos e processos de Tecnologia da Informação que visa atender às necessidades tecnológicas e de informação de um órgão ou entidade para um determinado período.

Política de Gestão de Riscos: declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos;

Probabilidade: medição do quanto provável é a ocorrência de um risco;

Risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos;

Riscos de Segurança: circunstância onde há probabilidade de que os ativos (pessoas, informações infraestrutura, produtos, imagem etc.) sejam alvo de um ataque bem-sucedido;

Riscos Estratégicos: riscos de longo prazo ou de oportunidade relacionados aos objetivos estratégicos e às estratégias adotadas para alcançá-los;

Risco Inerente: risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

Risco Residual: risco a que uma organização está exposta após a implementação de ações para o tratamento do risco.

Vulnerabilidade: fraqueza de um determinado ativo ou controle que pode ser explorado por uma ameaça.

7. ATIVIDADES E DESCRIÇÃO DAS ETAPAS

7.1. OBJETO DA GESTÃO DE RISCOS

Pode ser considerado objeto da gestão de riscos qualquer processo de trabalho, atividade, projeto, iniciativa, objetivos, resultados, metas, dados ou ação de plano, assim como os recursos que dão suporte à realização dos objetivos da DTI. É importante destacar que a gestão de riscos dos processos não dependerá exclusivamente do seu mapeamento, sendo necessário a participação de servidores/colaboradores/parceiros conhecedores do processo para levantamento dos principais riscos e as respectivas medidas mitigadoras.

Quanto aos projetos, todos precisam ter seus riscos geridos pelos seus respectivos gestores, conforme todas as etapas da sistemática de gestão dos riscos descritas nesta política.

A estrutura de gestão dos riscos na DTI dependerá da natureza e abrangência do objeto da gestão de riscos e precisa estar integrado ao **PDTI (2024-2026)**, uma vez que, os riscos constituem insumos para o diagnóstico do plano supracitado.

7.2. RISCOS DE TECNOLOGIA DA INFORMAÇÃO

Vários são os riscos que podem afetar negativamente o ambiente de Tecnologia da Informação na DTI do TCE-AL. Eles precisam ser tratados seguindo todo o ciclo do processo de gestão de riscos descrito abaixo no item 7.3 com a respectiva identificação do risco, possíveis causas, consequências e controles adotados para minimizar e/ou eliminar os impactos, conforme seguem:

Risco	Causa	Consequência	Controle
Falha humana relacionada ao manuseio do grupo gerador de energia	Acidente ao manusear equipamentos ou abastecimento do tanque de combustível	Interrupção no fornecimento de energia ao Data Center	Capacitação
Acesso físico não autorizado do Data Center	Falha nos controles de acesso físico ao Data Center	Indisponibilidade de recursos, serviços e sistemas informatizados; Roubo de informações	Cumprimento dos requisitos da Política de Controle de Acesso Lógico e Físico
Interrupção de energia elétrica	Fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 24horas; Fator interno que comprometa a rede elétrica do prédio como curtos-circuitos e infiltrações	Indisponibilidade de recursos, serviços e sistemas informatizados; Roubo de informações	Instalação e funcionamento de grupo gerador; Link redundante
Falhas ou queima de componentes eletrônicos	Oscilações elétricas	Indisponibilidade de recursos, serviços e sistemas informatizados; Perda de informações	Equipamentos redundantes
Indisponibilidade de backups 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	Não recuperação dos dados; Perda de dados	Estratégias de backup e restauração de dados

	backups		
Indisponibilidade de link de internet redundante	Inexistência de contrato de prestação de serviços de internet para link backup	Indisponibilidade de recursos, serviços e sistemas informatizados	Contrato de link 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	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 Armazenamento (storage) de dados	Indisponibilidade de rede de comunicação de dados;	Indisponibilidade de recursos, serviços e sistemas informatizados	Equipamentos redundantes;

	Oscilações de energia elétrica; Procedimento incorreto de configuração e acesso ao storage		Instalação e funcionamento de grupo gerador; Capacitações
Falhas ou erros no acesso à sistemas 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 recursos, serviços e sistemas informatizados; Perda de dados	Equipamentos redundantes; Instalação e funcionamento de grupo gerador; Capacitações

7.3. PROCESSO DE GESTÃO DE RISCO

O processo de gestão de riscos na DTI compreende as etapas de estabelecimento do contexto, a identificação, a análise, a avaliação, o tratamento, a comunicação e o monitoramento contínuo dos riscos a exemplo dos citados acima no item 7.2. Esse processo deve ser conduzido, preferencialmente, de forma coletiva, por meio de grupos compostos por pessoas que conheçam o objeto da gestão de riscos.

7.3.1. ESTABELECIMENTO DO CONTEXTO

Envolve o entendimento dos ambientes, interno e externo, em que o objeto de risco está inserido. Desta forma, é possível obter uma visão abrangente dos fatores que podem influenciar a unidade a atingir seus objetivos, bem como fornecer parâmetros e critérios para a definição de como as atividades subsequentes do processo de gestão de riscos serão conduzidas.

Esta etapa pode ser executada na seguinte sequência:

a) Identificar quais objetivos ou resultados devem ser alcançados;

b) Identificar os processos de trabalho relevantes para o alcance dos objetivos/resultados;

c) Identificar as pessoas envolvidas nesses processos e especialistas na área;

d) Mapear os principais fatores internos e externos que podem afetar o alcance dos objetivos/resultados (pessoas, sistemas informatizados, legislação, portarias, normativos, recursos, partes interessadas etc.);

e) Definir os objetos de gestão de risco mais importantes para a sua unidade ou trabalho.

7.3.2. IDENTIFICAÇÃO DOS RISCOS

Nesta etapa busca-se reconhecer e descrever os riscos que podem impactar os objetivos a serem alcançados, assim como, identificar as possíveis fontes de riscos. Para tanto, pode ser desenvolvida da seguinte forma:

a) Identificar com clareza o(s) objetivo(s)/resultado(s);

b) Listar, para cada objetivo/resultado, os eventos que possam vir a ter impacto negativo no alcance do objetivo/resultado;

c) Descrever como cada risco impacta o objetivo/resultado a ele associado.

Na identificação dos riscos é possível se basear em dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas. Neste sentido, recomenda-se a participação de pessoas com conhecimento adequado sobre o objeto de gestão de risco, utilizando ferramentas/técnicas que permitam reunir grande número de dados. São exemplos de técnicas/ferramentas: brainstorming, entrevistas, visitas técnicas, pesquisas etc. Neste ponto, destacamos a

importância de ser um processo inclusivo, em que as pessoas envolvidas manifestem sua ótica (quanto mais perspectivas da equipe, mais rico poderá ser o trabalho).

Auxiliam na identificação dos riscos:

a) Responder à seguinte pergunta-chave: o que pode atrapalhar o alcance do objetivo/resultado?

b) Considerar os fatores de sucesso para a obtenção dos objetivos (qualquer evento que afete o fator de sucesso potencialmente afeta o objetivo/resultado);

c) Considerar as principais fontes de riscos: infraestrutura, pessoal, processos, tecnologia, sistemas de TI e eventos externos.

7.3.3. ANÁLISE DOS RISCOS

A finalidade desta fase é compreender o risco e determinar o seu nível, de modo a subsidiar a sua análise e eventual tratamento.

A análise dos riscos deverá seguir os seguintes passos:

a) Avaliar o impacto do risco sobre o objetivo/resultado;

b) Avaliar a probabilidade de ocorrência do risco;

c) Definir o nível do risco com base na matriz probabilidade x impacto.

O impacto é o potencial que o risco tem de comprometer um objetivo, já a probabilidade é a chance desse evento ocorrer dentro do prazo previsto para se alcançar o resultado. Dessa forma, nível do risco é expresso em função dessas duas perspectivas.

Normalmente, são usadas escalas qualitativas de probabilidade e impacto, que podem assumir amplitudes variadas, dependendo do objeto e do grau de precisão na definição dos níveis.

A ferramenta mais indicada para combinar essas duas escalas e, a partir delas definir o nível do risco, é a matriz probabilidade x impacto, conforme segue na Tabela 1:

Probabilidade				
	Alta	Média	Alta	Alta
	Média	Baixa	Média	Alta
	Baixa	Baixa	**Baixa**	Média
		Insignificante	**Moderado**	**Crítico**
		Impacto		

a) Escala de Probabilidade (1 a 3):

1. Alta – ocorrência quase certa do risco comprometer um objetivo a ser alcançado;
2. Média – ocorrência de razoável frequência do risco comprometer um objetivo a ser alcançado;
3. Baixa – ocorrência de baixa frequência do risco comprometer um objetivo a ser alcançado.

b) Escala de Impacto (1 a 3):

1. Crítico – compromete totalmente o atingimento do objetivo/resultado;
2. Moderado – compromete razoavelmente o alcance do objetivo/resultado;
3. Insignificante – compromete minimamente o atingimento do objetivo/resultado.

Com base no nível do risco (cor), recomenda-se a adoção de uma postura de tratamento sugerida abaixo na Tabela 2:

Nível	Postura de Tratamento Sugerida
Alta	Riscos prioritários e exigem a definição e implantação imediata de ações corretivas.
Média	Riscos de média prioridade e requerem a definição e execução de ações corretivas para reduzir sua ameaça potencial.
Baixa	Riscos não graves onde recomenda-se apenas um monitoramento sistemático.

O objetivo da matriz de probabilidade x impacto consiste em ordenar os possíveis níveis de risco associadas a uma estimativa da probabilidade e impacto, bem como, facilitar a postura implementação das ações de contenção dos riscos. Cabe ressaltar que a dimensão do impacto é mais importante que a da probabilidade, uma vez que, é ele que compromete o atingimento do objetivo. Outro fator importante, nesta fase, é o conhecimento de todos pela gestão dos riscos e pelos processos de trabalhos a eles envolvidos, pois quanto maior o conhecimento, mais assertiva será a análise qualitativa.

7.3.4. AVALIAÇÃO DOS RISCOS

Na avaliação dos riscos é feita a comparação do seu nível com o limite de exposição a riscos (Item 6.2.3 - Tabela 1) com a finalidade de determinar se ele é aceitável e qual o tipo de tratamento é requerido (Item 6.2.3 - Tabela 2).

O limite de exposição a riscos representa o nível acima do qual, provavelmente, o risco necessitará de tratamento. O intuito é que, após o tratamento, o nível do risco real fique abaixo do limite de exposição. Esta avaliação contribui para a tomada de decisão em eventual tratamento do risco, porém não constitui em fator determinante, ou seja, cabe ao gestor decidir quais merecerão ações mitigadoras.

A avaliação dos riscos deverá seguir os seguintes passos:

a) Observar, na matriz probabilidade x impacto, os riscos cujos níveis estão acima do limite de exposição a risco (faixa vermelha);

b) Avaliar, para os riscos acima do limite, as respectivas fontes, causas e eventuais consequências sobre a organização como um todo;

c) Pontuar os riscos que estão abaixo do limite de exposição:

- ✓ Para os riscos cujos níveis se encontram na faixa amarela, deverá ser avaliada as ações direcionadas para reduzir as ameaças;
- ✓ Os riscos cujos níveis se encontram na faixa verde, a depender do cenário, poderão ser aceitos e sistematicamente monitorados.

7.3.5. TRATAMENTO DOS RISCOS

No tratamento dos riscos são realizados o planejamento e ações que modifiquem o nível do risco, por meio de respostas que mitiguem, transfiram ou evitem esses riscos, seguindo

diretrizes definidas nos procedimentos operacionais de **Gestão de Incidentes, Requisições e Mudanças**.

Vale salientar que serão apenas tratados os riscos priorizados, e a partir deles serão levantadas as fontes, causas e consequências associadas aos mesmos. A concepção de ações de respostas ao risco deve ser realizada por pessoas que conhecem bem o objeto de gestão de riscos, como também são recomendadas ferramentas que fomentem a identificação de maior quantidade de medidas de resposta, como brainstorming, visitas técnicas, pesquisas etc.

Normalmente o tratamento dos riscos segue as seguintes etapas:

a) Identificar as causas e consequências dos riscos priorizados;

b) A partir do levantamento das causas e das consequências, registrar as possíveis práticas de resposta ao risco;

c) Analisar a viabilidade da implantação dessas condutas (custo-benefício, viabilidade técnica, tempestividade, efeitos colaterais do tratamento etc.);

d) Decidir quais serão implementadas;

e) Elaborar plano de implementação das ações;

f) Monitorar os riscos atuais e tendências de novas riscos, bem como, revisar as ações de controle;

g) Fazer auditorias e revisões para as devidas adequações das medidas ao longo do tempo.

Na identificação das atividades de resposta ao risco, devem ser feitas as principais perguntas:

a) O que poderia ser feito para diminuir a probabilidade de ocorrência do risco?

b) O que poderia ser feito para diminuir impacto do risco no alcance do objetivo/resultado?

c) É possível fazer algo para eliminar e/ou transferir o risco?

Inicialmente, as ações devem se concentrar nas fontes e causas do risco (mitigadoras), para reduzir a probabilidade de ocorrência ou implantar planos de contingência que amenizem os impactos, na hipótese do risco se concretizar, ou uma combinação de ambos. Ao decidir implantar as práticas de resposta ao risco, devem ser considerados a quantidade e o nível dos riscos mitigados por cada ação adotada, assim como o grau de redução do nível do risco gerado.

São exemplos de ações mitigadoras a segregação de funções, as verificações prévias à contratação de terceiros, o redesenho de processos, a realocação de pessoas, a adoção de controles, a avaliação de desempenho, a realização de ações de capacitação, o desenvolvimento ou aperfeiçoamento de soluções de TI etc. Ademais, elas podem ser adotadas de forma isolada ou conjuntamente, sempre equilibrando os custos e os esforços com os benefícios decorrentes do tratamento.

As respostas aos riscos devem ser definidas e planejadas utilizando-se das seguintes estratégias:

Evitar: decidir em não iniciar ou descontinuar uma atividade ou processo que dá origem ao risco. Exemplo: A DTI decide se desfazer de uma atividade ou processo interno.

Reduzir: alterar o fator probabilidade com a implementação de controles específicos. Por exemplo, a DTI identifica e avalia o risco de seus sistemas permanecerem inoperantes por um período superior a três horas e decide não aceitar o impacto dessa ocorrência. Neste cenário resolve investir no aprimoramento de sistemas de autodetecção de falhas para reduzir a probabilidade de indisponibilidade dos sistemas.

Mitigar: alterar o fator impacto com a implementação de controles específicos. Por exemplo: A DTI pode investir na redundância dos equipamentos que processam as informações mais críticas para os seus processos. Havendo uma falha em algum desses equipamentos, a redundância implementada asseguraria a continuidade da operação dos respectivos sistemas, evitando o impacto nas atividades críticas.

Reter: manter o risco no nível atual de impacto e probabilidade. Por exemplo: A DTI decide não investir em melhorias na sua estrutura interna de informática, assumindo que as perdas e erros atualmente sabidos e esperados de informações internas para o processo de decisão e de gestão são impactos toleráveis.

Transferir: atividades que visam reduzir o impacto e/ou a probabilidade de ocorrência do risco através da transferência ou, em alguns casos, do compartilhamento de uma parte do risco. Por exemplo: A DTI identifica e avalia os riscos de falhas e desgaste natural dos veículos utilizados para transporte de equipamentos/materiais de TI. Após analisar a melhor estratégia a ser adotada no que tange às despesas possíveis com reparos e manutenção preventiva, licenciamentos, seguros e eventualmente até a paralisação de algumas atividades em função da indisponibilidade de veículos, decide terceirizar de forma que toda a manutenção, seguro e garantia de disponibilidade sejam de responsabilidade de um fornecedor externo, seguindo diretrizes definidas na **Política de Gestão de Fornecedores** e **Plano de Aquisições e Contratações de TI**.

Após a implementação da estratégia de tratamento selecionada, a efetividade dos controles colocados em prática deve ser avaliada em intervalos planejados e, em seguida, uma nova análise dos riscos a eles relacionados deve ser realizada, obtendo-se assim novas ações para tratar riscos residuais.

7.3.6. COMUNICAÇÃO DOS RISCOS

Como acontece em qualquer processo de gestão, a comunicação é atividade chave para a obtenção dos resultados esperados da gestão de riscos. É importante ressaltar que o processo de comunicação deve permear em toda DTI, proporcionando aos destinatários, dentro de suas respectivas funções e competências, informação indispensável à tomada de decisão quanto ao gerenciamento efetivo dos riscos.

7.3.7. MONITORAMENTO CONTÍNUO DOS RISCOS

O monitoramento contínuo 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.

A finalidade desta etapa é produzir informações confiáveis e tempestivas para a gestão dos riscos da DTI, de maneira que decisões possam ser tomadas a tempo e que os objetivos não sejam comprometidos por riscos não gerenciados. O monitoramento é atividade transversal a todas as outras atividades executadas, devendo ser inserido na rotina diária como forma de acompanhar e revisar a gestão de risco. Além disso, deve acompanhar o ciclo de planejamento funcionando nas seguintes dimensões:

a) No funcionamento da Gestão de Riscos na DTI;

b) Na implementação e nos resultados do tratamento de riscos;

c) Na evolução do nível dos riscos que não mereceram tratamento por parte das áreas gestoras.

O monitoramento da Gestão de Riscos na DTI ficará sob responsabilidade e supervisão dos Gestores da Governança e Segurança da Informação com a colaboração de todos, conforme diretrizes definidas **na Políticas Corporativa de Segurança da Informação**, **Privacidade e Proteção de Dados Pessoais** e **Governança de TI**. A gestão de riscos (processos, projetos, serviços de TI etc.) realizada em todos os níveis deve ser monitorada pelo responsável técnico de cada um deles. O controle dos riscos envolve a verificação contínua do funcionamento da implementação e dos resultados das ações mitigadoras, devendo considerar o tempo necessário para que elas produzam seus efeitos.

7.4. IMPORTÂNCIA DA CONSCIENTIZAÇÃO DA GESTÃO DE RISCOS

A conscientização sobre a Gestão de Riscos é fundamental em toda DTI para criar uma cultura resiliente, capaz de enfrentar desafios, garantir a continuidade dos negócios e aproveitar oportunidades de maneira eficaz e sustentável. Promover a conscientização sobre a gestão de riscos deve ser parte integrante da estrutura da Diretoria DTI, envolvendo treinamentos regulares, comunicação clara e a incorporação de práticas de gestão de riscos.

7.5. PENALIDADES

Violações à política supracitada estão sujeitas a sanções disciplinares estabelecidos nas normas, portarias e legislações vigentes, e serão decididas caso a caso pela Diretoria de Tecnologia e Informática.

7.6. CONSIDERAÇÕES FINAIS

O desenvolvimento da Gestão de Riscos na DTI do TCE-AL ocorrerá de maneira gradual, priorizando o levantamento e a gestão dos riscos inerentes aos processos mais críticos e respeitando a maturidade institucional quanto ao tema.

8. CONTROLE DE DOCUMENTOS E REGISTRO

Código	Responsável pela guarda	Permissão de acesso	Meio de arquivo	Indexação	Local de arquivo	Tempo de Arquivo	Forma de Disposição
PL-DTI-006	DTI	Restrito ao setor	Eletrônico	Alfabética	Base de Conhecimento	Permanente	Não aplicável

9. ANEXOS

Não se aplica.

10. HISTÓRICO DAS REVISÕES

Revisão	Descrição das alterações	Data
00	Emissão Inicial	06/06/2024
01	Formatação do texto conforme padrão de documento	10/06/2024
02	Readequação da Política com abrangência voltada apenas para a DTI do TCE-AL - Inclusão do item 1 – Introdução - Inclusão/ajustes de texto no item 2 – Objetivo - Inclusão/ajustes de texto no item 3 – Responsabilidades e Autoridades - Inclusão/ajustes de texto no item 4 – Abrangência - Inclusão/ajustes de texto no item 5 – Referências - Inclusão/ajustes de texto no item 6 – Conceitos e Definições - Inclusão/ajustes de texto no item 7 – Atividades e Descrição das Etapas do Processo de Gestão de Riscos - Inclusão do item 7.2 – Riscos em Tecnologia da Informação - Inclusão/ajustes de texto no item 7.3.5 – Tratamento dos Riscos - Inclusão/ajustes de texto no item 7.3.6 – Comunicação dos Riscos - Inclusão/ajustes de texto no item 7.3.7 – Monitoramento Contínuo dos Riscos	01/07/2024
03	Alterações no texto de acordo com as sinalizações pontuadas pela Governança Coordenação e demais Líderes de Serviços.	30/10/2024

Elaborado por: **Equipe de Processos e Projetos**	Analisado e Aprovado por: **Diretoria de TI**
Data da Elaboração: 06/06/2024	Data da Aprovação: