GABINETE DA PRESIDÊNCIA
Conselheiro José Carlos Novelli
Telefones: (65) 3613-7546 / 7577 / 7540 / 7542 / 7543
E-mail: presidencia@tce.mt.gov.br

INSTRUÇÃO NORMATIVA Nº 7/PRES/JCN/2023

Dispõe sobre a Política de Gestão de Risco de Tecnologia da Informação no âmbito do Tribunal de Contas do Estado de Mato Grosso.

O PRESIDENTE DO TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO, no uso de suas atribuições legais e regimentais que lhe são conferidas pelos incisos XXIV e LIII do art. 27, ambos do Regimento Interno deste Tribunal (aprovado pela Resolução Normativa nº 16/2021);

CONSIDERANDO a observância aos princípios constitucionais previstos no art. 37 da Constituição da República Federativa do Brasil de 1988 (CRFB/1988), em especial ao princípio da eficiência e ao princípio da economicidade, este último previsto no art. 70 da Carta Magna;

CONSIDERANDO o Plano Estratégico de Longo Prazo do Tribunal de Contas do Estado de Mato Grosso (TCE-MT) para o período de 2022-2027 e o seu Objetivo Estratégico nº 3 “Ampliar a eficiência dos processos internos do TCE-MT”, bem como o Indicador Estratégico nº 3.9 “Índice de governança da tecnologia da informação”;

CONSIDERANDO a Resolução Normativa nº 8/2022, que altera a Política de Segurança da Informação (PSI) no âmbito do TCE-MT;

CONSIDERANDO a Resolução Normativa nº 9/2022, que dispõe sobre a reestruturação e o funcionamento da Comissão de Governança de Tecnologia da Informação do TCE-MT, bem como a Portaria nº 127/2022, que institui o Comitê Gestor de Segurança da Informação, Privacidade e Proteção de Dados Pessoais do TCE-MT;

GABINETE DA PRESIDÊNCIA
Conselheiro José Carlos Novelli
Telefones: (65) 3613-7546 / 7577 / 7540 / 7542 / 7543
E-mail: presidencia@tce.mt.gov.br

CONSIDERANDO o Plano Diretor de Tecnologia da Informação proposto para 2024-2025;

CONSIDERANDO a proposta de reestruturação organizacional da Secretaria Executiva de Tecnologia da Informação;

CONSIDERANDO a ABNT NBR ISO 31000:2018, que estabelece normas de referência mundial em gestão de riscos e apresenta uma estrutura de trabalho e de processos para a gestão de diversos tipos de risco, abrangendo todas as organizações de qualquer segmento e tamanho;

CONSIDERANDO que as práticas organizacionais realizadas na instituição devem ser referência;

CONSIDERANDO as metodologias e os métodos das boas práticas de governança de tecnologia da informação a serem implantadas na Secretaria Executiva de Tecnologia da Informação;

CONSIDERANDO a necessidade de identificar, analisar, avaliar, priorizar, tratar e monitorar os eventos que possam impactar os objetivos e resultados propostos no Plano Estratégico para a Secretaria Executiva de Tecnologia da Informação;

CONSIDERANDO que os recursos são escassos e que cabe à Secretaria Executiva de Tecnologia da Informação zelar pela sua boa aplicação em soluções de tecnologia da informação alinhadas ao Plano Estratégico;

CONSIDERANDO que é competência da Comissão de Governança de Tecnologia da Informação do TCE-MT e de seu Comitê Gestor de Segurança da Informação, Privacidade e Proteção de Dados Pessoais revisar, atualizar e propor as normas, procedimentos, planos e/ou processos e

GABINETE DA PRESIDÊNCIA
Conselheiro José Carlos Novelli
Telefones: (65) 3613-7546 / 7577 / 7540 / 7542 / 7543
E-mail: presidencia@tce.mt.gov.br

instruções que regulamentem os princípios e valores existentes na Política de Segurança da Informação, com a finalidade de regulamentar e operacionalizar as diretrizes estabelecidas na Política de Segurança da Informação, na Política de Privacidade e Proteção de Dados Pessoais e na Política de Proteção de Dados Pessoais, todas deste Tribunal de Contas;

CONSIDERANDO a necessidade de implantar e implementar Política de Gestão de Risco de Tecnologia da Informação com métodos, procedimentos, práticas, normativas e regras alinhados aos conceitos modernos de caráter institucional aplicados à administração pública,

RESOLVE:

Art. 1º Instituir a Política de Gestão de Risco de Tecnologia da Informação no âmbito do TCE-MT.

DOS CONCEITOS

Art. 2º Para fins desta Instrução Normativa e efeitos da Política de Gestão de Risco de Tecnologia da Informação, são aplicadas as seguintes definições:

I – Risco: efeito da incerteza nos objetivos – sua mensuração se fundamenta em dois eixos principais, a probabilidade de ocorrência do evento que interfere nos objetivos e a magnitude dessa ocorrência em relação aos mesmos objetivos;

II – Tecnologia da Informação (TI): ativo estratégico que suporta processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, armazenar, disseminar e fazer uso de informações;

III – Gestão de risco em TI: conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção,

GABINETE DA PRESIDÊNCIA
Conselheiro José Carlos Novelli
Telefones: (65) 3613-7546 / 7577 / 7540 / 7542 / 7543
E-mail: presidencia@tce.mt.gov.br

implementação, monitoramento, análise crítica e melhoria contínua da gestão de risco em TI;

IV – Plano de Gestão de Risco de TI: documento da estrutura de gestão de risco de TI que especifica os recursos a serem aplicados aos riscos e aos seus componentes, como procedimentos, práticas, sequência e cronologia das atividades e atribuição de responsabilidades;

V – Governança de TI: mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão de TI, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade alinhadas ao Plano Estratégico da instituição;

VI – Gestão de TI: processos organizacionais, abrangendo o planejamento, execução, controle, ações corretivas e a utilização dos recursos colocados à disposição da Secretaria Executiva de Tecnologia e Informação para a consecução dos objetivos; preocupa-se com o dia a dia, no contexto das estratégias, políticas, processos e procedimentos estabelecidos e tem na eficácia (alcançar as metas) e na eficiência (utilização dos recursos disponíveis) seus maiores compromissos;

VII – Solução de Tecnologia da Informação: conjunto de sistemas, bens e serviços de TI que se integram visando ao atendimento das necessidades da instituição, devendo ser tratadas como ativo corporativo;

VIII – Plano Diretor de Tecnologia da Informação (PDTI): instrumento que viabiliza a entrega da solução em TI demandada, passando por sua identificação, análise e avaliação tecnológica, priorização, inclusão, tratamento orçamentário, procedimento de aquisição, recebimento, averiguação de conteúdo e encaminhamento à unidade gerencial solicitante;

IX – Plano de Continuidade de TI: plano que considera a gestão de risco de TI na sua formulação, com as estratégias a serem aplicadas e os planos de ação integrados, de forma a garantir a manutenção dos serviços de TI diante da manifestação de eventual situação de crise;

X – Comitê de Evolução Digital: unidade deliberativa para assuntos estratégicos na Secretaria Executiva de Tecnologia da Informação, componente

do sistema de instâncias internas de apoio à governança, proposta na reestruturação organizacional;

XI – Modelo de Três Linhas de Defesa: mecanismo que consiste em três níveis de proteção construídos para fornecer suporte redundante à gestão de risco e assegurar que eles sejam identificados e tratados previamente aos seus efeitos sobre os objetivos de TI;

XII – Nível de risco: resultado da interação entre a probabilidade de ocorrência do risco e do seu efeito sobre os objetivos;

XIII – Apetite a risco: nível de risco que a TI está disposta a aceitar;

XIV – Mapa de risco: documento onde são registrados os riscos identificados de acordo com a probabilidade de ocorrência e os efeitos esperados, possibilitando a elaboração das atividades necessárias à sua gestão.

DA FINALIDADE

Art. 3º A Política de Gestão de Risco de Tecnologia da Informação tem por finalidade estabelecer e disseminar práticas, métodos, procedimentos, normativas e regras aplicadas à TI que permitam, por meio de tomadas de decisão estratégicas, determinar os eventos que possam impactar o cumprimento da missão e dos objetivos institucionais, gerando riscos ou oportunidades.

Parágrafo único. A gestão de riscos de TI é parte componente do processo de planejamento estratégico de TI;

Art. 4º Esta Política de Gestão de Risco de Tecnologia da Informação se aplica à Secretaria Executiva de Tecnologia da Informação, não abrangendo a gestão de risco de outras unidades gerenciais do TCE-MT ou seus processos específicos.

DOS OBJETIVOS

GABINETE DA PRESIDÊNCIA
Conselheiro José Carlos Novelli
Telefones: (65) 3613-7546 / 7577 / 7540 / 7542 / 7543
E-mail: presidencia@tce.mt.gov.br

Art. 5º São objetivos da Política de Gestão de Risco de Tecnologia da Informação:

I – Assegurar que as incertezas que afetem o cumprimento dos objetivos propostos para a Secretaria Executiva de Tecnologia da Informação sejam identificadas, tratadas e monitoradas, minimizando ou anulando seus efeitos sobre esses objetivos e os resultados organizacionais esperados;

II – Garantir a disponibilidade e o funcionamento dos sistemas por meio de métricas e indicadores para analisar continuamente os riscos de TI;

III – Prover razoável segurança no cumprimento da missão e do negócio da Secretaria Executiva de Tecnologia da Informação;

IV – Fortalecer a integração entre as unidades gerenciais componentes da Secretaria Executiva de Tecnologia da Informação;

V – Subsidiar a tomada de decisão estratégica;

VI – Fomentar a cultura da identificação das oportunidades e ameaças setoriais e institucionais;

VII – Contribuir para a implementação do sistema de governança de TI;

VIII – Possibilitar a alocação eficiente dos recursos da instituição no tratamento dos riscos relacionados à TI;

IX – Auxiliar no estabelecimento de critérios e de parâmetros para os processos organizacionais de TI;

X – Possibilitar o incremento na capacidade da Secretaria Executiva de Tecnologia da Informação de se adaptar a alterações de cenários;

XI – Evitar desperdício de recursos.

DOS PRINCÍPIOS

Art. 6º São princípios da Política de Gestão de Risco de Tecnologia da Informação:

I – Elaboração da Metodologia da Gestão de Riscos de TI seguindo a do Planejamento Estratégico Institucional;

GABINETE DA PRESIDÊNCIA
Conselheiro José Carlos Novelli
Telefones: (65) 3613-7546 / 7577 / 7540 / 7542 / 7543
E-mail: presidencia@tce.mt.gov.br

II – Manutenção de fluxo regular e constante de dados e de informações entre as partes interessadas em gestão de risco de TI;

III – Observação da economicidade no tratamento dos riscos de TI;

IV – As contratações propostas no ambiente de gestão de risco de TI fazem parte do Plano Diretor de Tecnologia da Informação;

V – As demandas de solução em TI serão tratadas considerando os objetivos estratégicos da instituição, as necessidades setoriais e a gestão de risco de TI;

VI – Adequação a boas práticas de gestão de risco de TI, com normas, padrões e recomendações de referência;

VII – Alinhamento da gestão de riscos de TI aos padrões de ética institucional estabelecido;

VIII – Integração da gestão de riscos de TI aos processos organizacionais da Secretaria Executiva de Tecnologia da Informação;

IX – Transparência;

X – Melhoria dos processos de proteção e de segurança de TI.

DAS DIRETRIZES

Art. 7º São diretrizes da Política de Gestão de Risco de Tecnologia da Informação:

I – Capacitação como parte integrante do ciclo de aprendizado acerca da gestão de risco de TI;

II – Alinhamento com as melhores práticas reconhecidas para a gestão de risco de TI;

III – Comunicação tempestiva à Alta Direção dos riscos de TI identificados;

IV – Produção de informações de caráter estratégico por meio de diagnósticos, estudos e avaliações da gestão de risco de TI;

V – Avaliação, na mesma periodicidade do PDTI, da evolução da maturidade da gestão de risco de TI;

GABINETE DA PRESIDÊNCIA
Conselheiro José Carlos Novelli
Telefones: (65) 3613-7546 / 7577 / 7540 / 7542 / 7543
E-mail: presidencia@tce.mt.gov.br

VI – Aumento da eficiência operacional da Secretaria Executiva de Tecnologia da Informação

Art. 8º A instituição da Política de Gestão de Risco da Tecnologia da Informação está de acordo com o Indicador Estratégico nº 3.9 do Plano Estratégico de Longo Prazo do TCE-MT (2022-2027) e suas iniciativas, com destaque para a formulação dos riscos e das oportunidades no âmbito da Secretaria Executiva de Tecnologia da Informação e dos riscos nos contratos de TI.

Art. 9º A Política de Gestão de Risco de Tecnologia da Informação é parte integrante do Sistema de Governança estabelecido no âmbito da Secretaria Executiva de Tecnologia da Informação.

Art. 10º Cabe ao Secretário Executivo de Tecnologia da Informação liderar o macroprocesso de gestão de risco de tecnologia da informação.

DA METODOLOGIA DE GESTÃO DE RISCO DE TI

Art. 11 A gestão de risco de tecnologia da informação adotará as boas práticas estabelecidas na norma ABNT NBR ISO 31000:2018, ou a que vier a substituí-la, constituída dos seguintes processos:

I – Comunicação e consulta: atividade de conscientização das partes interessadas para o entendimento dos riscos (comunicação) e fornecimento de dados e informações necessárias para a tomada de decisão (consulta);

II – Estabelecimento do contexto: personalização do processo de gestão de risco – com a definição das atividades cobertas pelo escopo –, do contexto interno e externo e da quantidade e tipo de risco que podem ser suportados em relação aos objetivos da TI;

GABINETE DA PRESIDÊNCIA
Conselheiro José Carlos Novelli
Telefones: (65) 3613-7546 / 7577 / 7540 / 7542 / 7543
E-mail: presidencia@tce.mt.gov.br

III – Identificação dos riscos: atividade de identificar os riscos a partir dos objetivos propostos, utilizando metodologia específica, descrição com clareza dos possíveis riscos, suas fontes, vulnerabilidades e consequências;

IV – Análise dos riscos: atividade realizada para determinar os níveis de risco a partir da matriz de probabilidade e impacto;

V – Avaliação dos riscos: comparação dos resultados da análise de risco com os limites ao risco adotados nos níveis de tolerância a risco;

VI – Tratamento dos riscos: resposta ao risco a partir de seleção de opções para sua abordagem, considerando o nível de risco identificado, com a devida avaliação da eficácia;

VII – Monitoramento e análise crítica: práticas de observação e análise do atendimento aos padrões estabelecidos para identificar mudanças no contexto da TI, analisar o aprendizado e fomentar a melhoria contínua, visando subsidiar a gestão sobre o desempenho das medidas adotadas.

Art. 12 Os níveis de risco a serem considerados nesta Política de Gestão de Risco de Tecnologia da Informação são:

I – Risco alto/extremo: nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser comunicado à governança e à Alta Administração e ter uma resposta imediata. Postergação de medidas só com autorização do dirigente máximo;

II – Risco médio: nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da gerência na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais;

III – Risco baixo: nível de risco dentro do apetite a risco, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo mais riscos, avaliando a relação custos x benefícios, como diminuir o nível de controles.

GABINETE DA PRESIDÊNCIA
Conselheiro José Carlos Novelli
Telefones: (65) 3613-7546 / 7577 / 7540 / 7542 / 7543
E-mail: presidencia@tce.mt.gov.br

Art. 13 O Plano de Gestão de Risco da Tecnologia da Informação contribui para a identificação de possíveis ameaças que possam afetar os objetivos de TI, especificando os controles, a estrutura, a criticidade, a matriz e o nível de risco, a definição do apetite a risco, a tolerância e o tratamento dos riscos.

Art. 14 Nas atividades de planejamento estratégico da Secretaria Executiva de Tecnologia da Informação devem ser considerados, no que couber, riscos e oportunidades como requisitos para a seleção e priorização de objetivos, indicadores, metas, estratégias e iniciativas.

Art. 15 A Política de Gestão de Risco da Tecnologia da Informação adotará o Modelo de Três Linhas de Defesa, mecanismo eficaz para melhorar a comunicação e o controle por meio da definição das atribuições e responsabilidades específicas de cada unidade ou profissional dentro da TI, para que cada um entenda os seus papéis e limites e como seus cargos se encaixam na estrutura de gestão de risco e controle.

I – 1ª linha de defesa: gestão operacional, com o controle da gerência ou do gestor, responsável por implementar as ações corretivas para resolver deficiências em processos e controles, por manter controles internos eficazes e por conduzir procedimentos de riscos e controle. Devem identificar, avaliar, controlar e mitigar os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos e garantindo que as atividades estejam de acordo com as metas e objetivos. São as funções que gerenciam e têm propriedade de riscos;

II – 2ª linha de defesa: com funções de controle de riscos e supervisão de conformidade, as unidades de segunda linha de defesa estão situadas no nível de gestão. A gerência estabelece diversas funções de gerenciamento de riscos e conformidade para ajudar a desenvolver e/ou monitorar os controles da primeira linha de defesa;

III – 3ª linha de defesa: é a auditoria interna, com avaliação independente, para fornecimento à governança de TI e à Alta Administração de avaliações abrangentes baseadas no maior nível de independência e objetividade sobre a eficácia da gestão de risco de TI e dos controles internos, incluindo a forma como a primeira e a segunda linhas de defesa alcançam os objetivos de gerenciamento de riscos e controle.

Art. 16 A utilização do Modelo de Três Linhas de Defesa na gestão de risco de TI determina a segregação das funções críticas e das responsabilidades fundamentais.

Art. 17 A Secretaria Executiva de Tecnologia da Informação terá unidade gerencial específica para a gestão de risco de TI para desempenhar, entre outras, as seguintes atribuições:

I – Realizar e consolidar a análise de riscos de aquisição de produtos e serviços de TI, incluindo sua viabilidade;

II – Propor e acompanhar a destinação de recursos orçamentários adequados para realização das estratégias de TI;

III – Sugerir mecanismos para a elaboração do Plano de Contratação Anual e do Plano de Continuidade e Contingência, com as considerações pertinentes;

IV – Acompanhar os relatórios de conformidade de execução dos contratos de TI elaborados pelos fiscais;

V – Apoiar os estudos técnicos de contratação de serviços e aquisições de TI;

VI – Sugerir ações de modernização e automação dos macroprocessos de TI.

Art. 18 Compete ao Comitê de Evolução Digital, instância interna de apoio à governança na Secretaria Executiva de Tecnologia da Informação, liderar e coordenar a elaboração, implantação e implementação do Plano Diretor

GABINETE DA PRESIDÊNCIA
Conselheiro José Carlos Novelli
Telefones: (65) 3613-7546 / 7577 / 7540 / 7542 / 7543
E-mail: presidencia@tce.mt.gov.br

de TI, do Plano de Gestão de Risco de TI e do Plano de Continuidade e Contingência, entre outras responsabilidades.

Art. 19 O Plano Diretor de Tecnologia da Informação, instrumento que formaliza o planejamento de TI no TCE-MT, a ser elaborado pela Secretaria Executiva de Tecnologia da Informação, conterá, entre outros itens, o Plano de Gestão de Riscos de TI e o Plano de Continuidade e Contingência de TI.

Art. 20 Esta Instrução Normativa entra em vigor na data de sua publicação.

Publique-se. Registra-se. Cumpra-se.

(assinatura digital)
CONSELHEIRO JOSÉ CARLOS NOVELLI
Presidente do TCE-MT