MINUTA

Instrução Normativa Nº xxx/2023, de xxx de agosto de 2023

Dispõe sobre a Política de Gestão de Riscos de Tecnologia da Informação e aprova o de Plano de Gestão de Riscos de TI no âmbito do Tribunal Regional Eleitoral do Acre.

O Presidente do Tribunal Regional Eleitoral do Acre, no uso de suas atribuições legais e,

TENDO EM VISTA o disposto no Art. 37 da Resolução CNJ nº 370/2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

TENDO EM VISTA a Resolução n. 1.722/2017 que dispõe sobre a política de gestão de riscos no âmbito do Tribunal Regional Eleitoral do Acre;

TENDO EM VISTA a Resolução n. 1.727/2018 que aprova a Metodologia de Gestão de Riscos no âmbito do Tribunal Regional Eleitoral do Acre;

TENDO EM VISTA a Resolução n. 1.776/2022 que implementa, no âmbito do Tribunal Regional Eleitoral do Acre, a Resolução TSE n. 23.644/2021, que estabelece a Política de Segurança da Informação da Justiça Eleitoral;

TENDO EM VISTA as normas da Associação Brasileira de Normas Técnicas - ABNT NBR ISO 27.005:2011, 31.000:2018 e 31.010:2019, que tratam de princípios, diretrizes e técnicas relacionados ao processo de gestão de riscos;

TENDO EM VISTA as boas práticas preconizadas nos Objetivos de Controle para Informação e Tecnologias Relacionadas (*Control Objectives for Information and related Technology* – COBIT 5);

RESOLVE:

Art. 1° Instituir, no âmbito do Tribunal Regional Eleitoral do Acre, a Política de Gestão de Riscos de Tecnologia da Informação e aprovar o Plano de Gestão de Riscos de TI, descrito no anexo único desta Instrução Normativa.

Art. 2º A Política de Gestão de Riscos de Tecnologia da Informação do Tribunal Regional Eleitoral do Acre compreende os objetivos, os princípios, as diretrizes e as responsabilidades relacionadas à Gestão de Riscos de TI.

Art. 3º A Gestão de Riscos de Tecnologia da Informação é um processo contínuo e iterativo que visa identificar, avaliar, mitigar e controlar os riscos que podem afetar os objetivos institucionais, bem como oferecer maior garantia para o sucesso do negócio, fornecendo uma estrutura para gerenciar os riscos associados à tecnologia da informação.

CAPÍTULO I

DAS DEFINIÇÕES

Art. 4º Para fins desta Resolução, considera-se:

I - análise crítica: técnica de levantamento de informações acerca de processos e sistemas utilizados na instituição de modo a melhorar a governança de ativos de TI em relação às vulnerabilidades que podem ser encontradas, verificando a probabilidade de ocorrência de determinados eventos e as consequências que eles podem trazer.

II - apetite a riscos: nível de risco de forma qualitativa que o TRE-AC está disposto a aceitar;

III - avaliação de riscos: processo global de identificação, análise e avaliação de riscos;

IV - Comitê Gestor de Tecnologia da Informação (CGTIC): equipe técnica composta pelo secretário e coordenadores da Secretaria de Tecnologia da Informação;

V - Comitê Setorial (COSET): equipe multidisciplinar integrada por participantes da alta administração do TRE-AC, designada para deliberar sobre políticas, diretrizes e investimentos na área de Tecnologia da Informação;

VI - 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;

VII - fonte de risco: elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco;

VIII - Gestão de Riscos de Tecnologia da Informação: atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos de Tecnologia da Informação;

IX - identificação de riscos: processo de busca, reconhecimento e descrição de riscos;

X - nível de risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das probabilidades e dos seus impactos;

XI - Plano de Gestão de Riscos: esquema (plano) dentro da estrutura de gestão de riscos, que especifica a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos;

XII - Processo de Gestão de Riscos: aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e de identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos;

XIII - proprietário de risco: pessoa ou entidade com responsabilidade e autoridade para gerenciar um risco;

XIV - resposta a risco: qualquer ação adotada para lidar com risco, podendo consistir em:

a) aceitar o risco por uma escolha consciente;

b) transferir ou compartilhar o risco;

c) evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco; ou

d) mitigar ou reduzir o risco diminuindo sua probabilidade de ocorrência ou minimizando suas consequências;

XV - risco: evento ou condição incerta que, se ocorrer, provocará um efeito positivo ou negativo nos objetivos estabelecidos;

XVI - risco residual: risco remanescente após o tratamento do risco;

XVII - tratamento de riscos: processo de estipular uma resposta a risco;

XVIII - vulnerabilidade: na tecnologia da informação o termo se refere a uma falha ou fraqueza em programas, sistemas, redes ou dispositivos informatizados que pode ser explorada por um atacante para obter acesso não autorizado, bem como causar danos e prejuízos.

CAPÍTULO II

DOS OBJETIVOS

Art. 5º A Política de Gestão de Riscos de Tecnologia da Informação em como objetivo geral subsidiar a tomada de decisão baseada na análise de riscos, com vistas a prover a Administração de razoável segurança no cumprimento da sua missão e no alcance dos seus objetivos institucionais, estabelecendo princípios, diretrizes e responsabilidades.

Art. 6º São objetivos específicos da Política de Gestão de Riscos de Tecnologia da Informação:

I - identificar eventos com potencial para afetar o atingimento dos objetivos institucionais;

II – fortalecer as decisões em resposta aos riscos de Tecnologia da Informação;

III – aprimorar os controles internos administrativos.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 7º São princípios da Política de Gestão de Riscos de Tecnologia da Informação do TRE-AC:

I - estar alinhada ao Planejamento Estratégico Institucional;

II - estar alinhada ao Planejamento Estratégico de Tecnologia da Informação (PETI);

III - estar alinhada ao Plano Diretor de Tecnologia da Informação (PDTI);

IV – estar alinhada a Política de Gestão de Riscos;

V – abordar especificamente o efeito da incerteza nos objetivos estabelecidos de forma que a natureza e a fonte da incerteza sejam devidamente compreendidas para que o risco possa ser avaliado ou tratado com sucesso;

VI – ser sistemática, estruturada e oportuna;

VII – considerar fontes de informações tempestivas e confiáveis, para que a tomada de decisão seja fundamentada mediante a análise crítica dos riscos;

VIII – considerar a importância dos fatores humanos e culturais;

IX – envolver, de forma transparente, apropriada e oportuna, todos os níveis da organização;

X – ser dinâmica, interativa e capaz de perceber e reagir às mudanças, respondendo-as tempestivamente;

XI – promover a melhoria contínua, desenvolvendo e implementando estratégias para que o Tribunal implemente oportunidades de aprimoramento.

CAPÍTULO IV

DAS DIRETRIZES

Art. 8º A Gestão de Riscos de Tecnologia da Informação observará as seguintes diretrizes:

I – comunicação clara e objetiva a todas as partes interessadas dos resultados de cada uma das etapas do processo de gestão de riscos de TI;

II – integração de tecnologia, processos e pessoas;

III – observação das melhores práticas de governança e de gestão de riscos de TI;

IV – razoabilidade da relação custo-benefício nas ações existentes no plano de resposta aos riscos de TI;

V – participação da alta administração na gestão dos riscos.

CAPÍTULO V

DOS ELEMENTOS ESTRUTURAIS

Art. 9º São elementos estruturais da Política Gestão de Riscos de Tecnologia da Informação no TRE-AC:

I - o Processo de Gestão de Riscos de TI;

II – o Plano de Gestão de Riscos de TI;

Parágrafo único. Com base em informações obtidas pelo monitoramento e análise crítica dos riscos, os elementos estruturais da Gestão de Riscos de TI devem ser constantemente aprimorados para melhorar o processo e tornar o Tribunal mais resiliente aos riscos de TI.

CAPÍTULO VI

DAS RESPONSABILIDADES

Art. 10º A Gestão de Riscos de Tecnologia da Informação é parte integrante dos processos organizacionais afetos à área de Tecnologia da Informação e constitui responsabilidade:

I - do proprietário do risco de TI, em primeira instância;

II - do Comitê Gestor de TI (CGTIC), em segunda instância;

III - do Comitê Setorial (COSET), em terceira instância.

§ 1º A Assistência de Planejamento e Governança de Tecnologia da Informação (ASPGOVTI) deverá prestar apoio nas atividades relacionadas à Gestão de Riscos de TI.

§ 2º A Coordenadoria de Controle Interno (COCIN) deverá atuar como orientadora e fiscalizadora do processo de Gestão de Riscos de Tecnologia da Informação.

Art. 11. Compete ao proprietário do risco de Tecnologia da Informação:

I - gerir os riscos de TI sob sua responsabilidade;

II – submeter ao CGTIC os riscos de TI que extrapolarem sua competência e capacidade de gerenciamento;

III - encaminhar à ASPGOVTI o Plano de Gestão dos Riscos de TI sob sua responsabilidade.

Art. 12. Compete ao CGTIC:

I - revisar esta Política de Gestão de Riscos de Tecnologia da Informação e apresentar proposta de alteração ao COSET;

II - operacionalizar, no âmbito das unidades da STI, a aplicação dos recursos disponibilizados para a gestão de riscos;

III - dirimir eventuais dúvidas dos proprietários de risco, na execução do processo de Gestão de Riscos de Tecnologia da Informação;

IV - deliberar sobre os riscos considerados médios e altos que, eventualmente, lhe forem apresentados pelos proprietários de risco;

V - submeter ao COSET, acompanhados de manifestação, os riscos de Tecnologia da Informação considerados extremos e os riscos residuais considerados altos;

VI - subsidiar o COSET com informações técnicas, visando auxiliá-lo no processo de tomada de decisão;

VII - revisar continuamente o modelo do processo de Gestão de Riscos de TI e submetê-lo à aprovação do COSET;

VIII - conscientizar os gestores sobre a importância da gestão de riscos de TI e a responsabilidade inerente a cada proprietário dos riscos.

Art. 13. Compete ao COSET:

I - aprovar a Política de Gestão de Riscos de TI;

II - promover a revisão periódica e a atualização desta Política de Gestão de Riscos de TI;

III - assegurar a alocação dos recursos necessários à Gestão de Riscos de TI;

IV - avaliar a adequação, a suficiência e a efetividade da Política de Gestão de Riscos de TI;

V - deliberar, após manifestação do Comitê Gestor de TI, sobre os riscos de TI considerados extremos e os riscos residuais considerados altos, que lhe forem submetidos pelo CGTIC;

Art. 14. Compete à Assistência de Governança de Tecnologia da Informação:

I - proceder à integração dos planos de gestão de riscos de TI a ela encaminhados, monitorando os riscos e reportando-os ao CGTIC, periodicamente;

II - divulgar e auxiliar à implementação e à operacionalização do processo de gerenciamento de riscos de TI nas unidades, equipes e comissões relacionadas à STI;

III - propor ao CGTIC melhorias para o processo e para esta Política de Gestão de Riscos de TI e para o processo correspondente.

Art. 15. Compete à Coordenadoria de Controle Interno, no âmbito de suas atribuições:

I - incluir, nos planos de auditoria, ações de avaliação do gerenciamento de riscos de TI;

II - utilizar as ferramentas e técnicas de auditoria interna para analisar riscos e controles administrativos na área de TI;

III - avaliar os controles internos utilizados pela STI na gestão de seus riscos;

IV - realizar auditorias periódicas com vistas a aferir o atendimento das diretrizes formuladas para a Gestão de Riscos de TI e a efetividade da Política de Gestão de Riscos de Tecnologia da

Informação.

CAPÍTULO VI

DO PLANO DE GESTÃO DE RISCOS DE TI

Art. 16. O Plano de Gestão de riscos de TI mencionado no art. 1º e descrito no anexo único desta norma estabelece um conjunto de procedimentos a serem adotados no gerenciamento dos riscos de Tecnologia da Informação no âmbito deste Tribunal,

Parágrafo 1º. O Plano mencionado no caput deverá ser utilizado como referência para a identificação, a análise, a avaliação, o tratamento, a priorização, o monitoramento e a comunicação de riscos de Tecnologia da Informação, relativos aos objetivos e iniciativas estratégicas, bem como as ações a eles inerentes, da área de TI do Tribunal em conformidade com definições, priorizações e determinações estabelecidas pelo Comitê Setorial (COSET).

Art. 17. O Plano de Gestão de Riscos de TI deverá ser alinhado continuamente ao Processo de Gestão de Riscos de TI estabelecido no âmbito deste Tribunal e às normas da Associação Brasileira de Normas Técnicas – ABNT vigentes, sem prejuízo da aplicação de outras normas complementares.

Parágrafo único. A modelagem do Processo de Gestão de Riscos de Tecnologia da Informação deverá ser elaborada pelo CGTIC e publicada em até noventa dias, após a publicação desta Política.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 18. Esta Política e o Plano de Gestão de Riscos de TI, deverão ser revisados, no máximo, a cada 2 (dois) anos, ou a qualquer tempo, quando necessário.

Art. 19. Os casos omissos ou excepcionais serão resolvidos pelo COSET.

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