TRIBUNAL REGIONAL ELEITORAL DE RONDÔNIA

RESOLUÇÃO N. 20/2019

Instrução n. 0600238-85.2019.6.22.0000 – Classe 19 - Porto Velho - RO

Relator: Desembargador Sansão Saldanha

Interessado: Tribunal Regional Eleitoral de Rondônia

Dispõe sobre a Política de Gestão de Riscos de Tecnologia da Informação e Comunicação do Tribunal Regional Eleitoral de Rondônia.

O TRIBUNAL REGIONAL ELEITORAL DE RONDÔNIA no uso de suas atribuições legais;

CONSIDERANDO as orientações do Tribunal de Contas da União (TCU), constantes nas decisões normativas que regulamentam a elaboração anual dos relatórios de gestão das unidades jurisdicionadas, no que se refere ao aprimoramento das estruturas de governança e de controle da gestão; Acórdão TCU nº 2.467/2013; Acórdão TCU 2.524/2015; Acórdão TCU nº 2.604/2018 e Acórdão TCU nº 2.681/2018, todos do Plenário;

CONSIDERANDO as normas ABNT NBR ISO/73:2009, 27.005:2011, 31.000:2009 e 31.010:2012, que, respectivamente, fornece as definições de termos genéricos relativos à gestão de riscos; fornecem diretrizes para o processo de gestão de riscos de segurança da informação; estabelece princípios e diretrizes genéricas para a gestão de riscos; e fornece orientações sobre a seleção e a aplicação de técnicas sistemáticas para o processo de avaliação de riscos;

CONSIDERANDO as boas práticas preconizadas pelo guia internacional COBIT-2019, voltadas ao alcance dos objetivos descritos como: Otimização de Riscos Assegurada (EDM03) e Riscos Gerenciados (APO12);

CONSIDERANDO os princípios e diretrizes genéricas, contidos na Política de gerenciamento de riscos instituída por meio da Resolução TRE-RO nº 05/2017;

RESOLVE:

Art. 1º Instituir a Política de Gestão de Riscos de Tecnologia da Informação e Comunicação do Tribunal Regional Eleitoral de Rondônia, nos termos desta Resolução, que compreende:

I – Objetivos da Política de Gestão de Riscos;

II – Princípios da Gestão de Riscos;

III – Diretrizes da Gestão de Riscos;

IV – Responsabilidades.

Art. 2º A Gestão de Riscos constitui processo corporativo contínuo e iterativo, que visa dirigir e controlar eventos que possam afetar o cumprimento dos objetivos institucionais, oferecendo maior garantia para o sucesso do negócio.

CAPÍTULO I

DAS DEFINIÇÕES

Art. 3º Para fins desta Resolução, considera-se:

1. Apetite a riscos: quantidade e tipo de riscos que a organização está preparada para reter ou assumir;

2. Análise crítica: atividade realizada para determinar a adequação, a suficiência e a eficácia do assunto em questão para atingir os objetivos estabelecidos;

3. 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;

4. Comitê Executivo de Tecnologia da Informação e Comunicação (CETIC): equipe técnica formada pelos gestores da unidade de TIC, oficialmente

designada para deliberar sobre planos táticos e operacionais de TIC, em conformidade com a norma que o define**;**

5. Comitê Diretivo de Tecnologia da Informação e Comunicação (CDTIC): equipe multidisciplinar, oficialmente designada para deliberar sobre políticas, diretrizes e investimentos em TIC, em conformidade com a norma que o define;

6. Consequência: resultado de um evento que afeta os objetivos estabelecidos;

7. Contexto: conjunto de fatores internos e externos à organização que, juntamente com os critérios de riscos, definirão o ambiente de gerenciamento dos riscos;

8. 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;

9. Fonte de risco: elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco;

10. Gestão de riscos: atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos;

11. Impacto: grandeza ou dimensão das consequências ou efeitos da ocorrência de um evento;

12. Nível de risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das probabilidades e dos seus impactos;

13. Parte interessada: pessoa ou organização que pode afetar, ser afetada, ou perceber–se afetada por uma decisão ou atividade;

14. Plano de gestão de riscos: esquema dentro da estrutura de gestão de riscos, que especifica a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos;

15. Probabilidade: chance de algo acontecer;

16. Processo de avaliação de riscos: processo global de identificação, análise e avaliação de riscos;

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

18. Proprietário de risco: pessoa ou entidade com responsabilidade e autoridade para gerenciar um risco;

16. Risco: evento ou condição incerta que, se ocorrer, provocará um efeito positivo ou negativo nos objetivos estabelecidos;

20. Riscos residuais: risco remanescente após o tratamento do risco;

21. Vulnerabilidade: propriedades intrínsecas de algo resultando em suscetibilidade a uma fonte de riscos que pode levar a um evento com uma consequência.

CAPÍTULO II

DOS OBJETIVOS DA POLÍTICA DE GESTÃO DE RISCOS

Art. 4º A Política de Gestão de Riscos tem por objetivo geral estabelecer princípios, diretrizes e responsabilidades para a gestão de riscos, incorporando a visão de riscos à tomada de decisão, em conformidade com as melhores práticas adotadas no setor público.

Art. 5º A Política de Gestão de Riscos tem por objetivos específicos promover:

I - a identificação de eventos em potencial que afetem a consecução dos objetivos institucionais;

II - o fortalecimento das decisões em resposta aos riscos;

III - o aprimoramento dos controles internos administrativos.

CAPÍTULO III

DOS PRINCÍPIOS DA GESTÃO DE RISCOS

Art. 6º A Gestão de Riscos adotada observará os seguintes princípios:

I - criar e proteger valores institucionais;

II - ser parte integrante dos processos organizacionais;

III - ser parte da tomada de decisões;

IV - abordar explicitamente a incerteza;

V - ser sistemática, estruturada e oportuna;

VI - ser baseada nas melhores informações disponíveis;

VII - estar alinhada ao contexto da instituição;

VIII - considerar fatores humanos e culturais;

IX - ser transparente e inclusiva;

X - ser dinâmica, iterativa e capaz de reagir a mudanças;

XI - facilitar a melhoria contínua da organização.

CAPÍTULO IV

DAS DIRETRIZES PARA A GESTÃO DE RISCOS

Art. 7º O processo de gestão de riscos contempla o estabelecimento do contexto, a identificação, a análise, a avaliação, o tratamento de riscos, a comunicação e consulta com partes interessadas, o monitoramento e a melhoria contínua.

§ 1º O estabelecimento do contexto consiste em compreender o ambiente externo e interno no qual o objetivo de gestão de riscos encontra-se inserido e em identificar parâmetros e critérios a serem considerados no processo de gestão de riscos.

§ 2º A identificação do risco compreende o reconhecimento e descrição dos riscos relacionados a um objeto de gestão, envolvendo a identificação de possíveis fontes de riscos, eventos, causas e consequências.

§ 3º A análise do risco refere-se ao desenvolvimento da compreensão sobre o risco e à determinação do nível do risco.

§ 4º A avaliação do risco envolve a comparação do nível do risco com critérios, a fim determinar se o risco é aceitável.

§ 5º O tratamento do risco compreende o planejamento e a realização de ações para modificar o nível do risco.

§ 6º O monitoramento 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.

§ 7º A comunicação e consulta refere-se à identificação das partes interessadas em objetos de gestão de riscos e obtenção, fornecimento ou compartilhamento de informações relativas à gestão de riscos sobre tais objetos, observada a classificação da informação quanto ao sigilo.

§ 8º A melhoria contínua compreende o aperfeiçoamento ou ajuste de aspectos da gestão de riscos avaliados no monitoramento.

Art. 8º O processo de gestão de riscos de TIC deve observar:

I - o ambiente interno e externo à unidade de TIC;

II - os objetivos estratégicos, táticos e operacionais;

III - a razoabilidade da relação custo-benefício nas ações para tratamento de riscos;

IV - a comunicação tempestiva sobre riscos às partes interessadas;

V - o acompanhamento dos riscos à segurança da informação, aos serviços judiciais e aos ativos críticos de TIC pelas instâncias de governança do TRE-RO;

Parágrafo único. Nas atividades de planejamento, considera-se, sempre que couber, o risco como um dos critérios para seleção e priorização de iniciativas e ações.

CAPÍTULO V

DAS RESPONSABILIDADES PELA GESTÃO DE RISCOS

Art. 9º A Gestão de Riscos é parte integrante dos processos organizacionais afetos à TIC e constitui responsabilidade:

I - Em primeira instância, do proprietário do risco;

II - Em segunda instância, do CETIC;

III - Em terceira instância, do CDTIC.

§1º - O comitê de gestão de riscos da Justiça Eleitoral de Rondônia deverá atuar como apoio à Gestão de Riscos de TIC.

§2º - A unidade de Controle Interno e Auditoria ou equivalente deverá atuar como orientadora do processo de Gestão de Riscos de TIC, nos termos da Resolução TRE-RO nº 5/2017.

Art. 10 Compete ao proprietário de risco:

I - Gerir os riscos sob sua responsabilidade.

II – Reportar ao CETIC os riscos que eventualmente extrapolarem sua competência e capacidade para gerenciamento;

III – Encaminhar ao comitê de gestão de riscos, os Planos de Gestão de Riscos de TIC de sua responsabilidade.

Art. 11 Compete ao CETIC:

I – Revisar esta Política de Gestão de Riscos de TIC e apresentar proposta de alteração e/ou atualização ao CDTIC;

II – Operacionalizar, no âmbito das unidades de TIC, 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 TIC;

IV – Deliberar sobre os riscos considerados médios e altos que, eventualmente, lhes forem apresentados pelos proprietários de risco;

V – Submeter ao CDTIC, após sua apreciação e manifestação, os riscos considerados extremos e os riscos residuais considerados altos;

VI – Subsidiar o CDTIC com informações técnicas, visando auxiliá-lo no processo de tomada de decisão;

VII – Elaborar o modelo do processo de Gestão de Riscos de TIC, e submetê-lo à aprovação do CDTIC.

Art. 12 Compete ao CDTIC:

I – Definir o apetite a riscos;

II - Avaliar, previamente à aprovação pela autoridade competente, a minuta da Política de Gestão de Riscos de TIC e suas revisões;

III - Assegurar a alocação dos recursos necessários à gestão de riscos de TIC;

IV – Avaliar a adequação, a suficiência e a eficácia da Estrutura de Gestão de Riscos de TIC;

V – Deliberar, após apreciação do CETIC, sobre os riscos considerados extremos e os riscos residuais considerados altos, que lhe forem submetidos por aquele Comitê Executivo;

VI – Aprovar o modelo do processo de Gestão de Riscos de TIC, elaborado pelo CETIC.

CAPÍTULO VI

DAS DISPOSIÇÕES GERAIS

Art. 13 Como modelo de referência para o processo de gestão de riscos de TIC, o Tribunal adotará aquele estabelecido na norma ABNT NBR ISO 31000:2009, sem prejuízo da aplicação de outras normas complementares.

Art. 14 Os casos omissos ou excepcionais serão resolvidos pelo CDTIC.

Art. 15 Esta Resolução entra em vigor na data de sua publicação.

Porto Velho, 18 de setembro de 2019.

Desembargador SANSÃO SALDANHA

Presidente e Relator

RELATÓRIO

O SENHOR JUIZ SANSAO BATISTA SALDANHA: Os autos em tela compreendem a reunião dos documentos encartados no Processo SEI n. 0001657-51.2019.6.22.8000, instaurado com a finalidade de materializar os atos necessários à implantação e regulamentação da Política de Gestão de Riscos de Tecnologia da Informação e Comunicação deste Tribunal Regional Eleitoral de Rondônia.

Da leitura dos autos, infere-se que a adoção da política em comento permite um claro delineamento de seus objetivos, princípios, diretrizes e responsabilidades, tratando-se, portanto, de uma importante ferramenta de gestão.

Concluído o exame dos autos e estando de acordo com os termos da proposta de resolução apresentada pelo Comitê Executivo de Tecnologia da Informação e Comunicação (CETIC - evento SEI 0439406), voto pela sua aprovação e submeto a matéria ao conhecimento e deliberação dos eminentes pares.

VOTO

O SENHOR JUIZ SANSAO BATISTA SALDANHA (Relator): Como dito preambularmente, o processo em tela foi autuado com a finalidade de compilar os atos e documentos necessários à regulamentação da Política de Gestão de Riscos de Tecnologia da Informação e Comunicação deste Tribunal, com estudo inicial deflagrado pela Seção de Governança e Controle – SEGOV. Referido material encontra fundamento nas orientações do Tribunal de Contas da União (TCU), normas ABNT NBR ISO/73:2009, 27.005:2011, 31.000:2009 e 31.010:2012 e princípios e diretrizes genéricas contidos na política de gerenciamento de riscos instituída por meio da Resolução TRE-RO nº 05/2017 (Processo SEI n. 0001657-51.2019.6.22.8000 – evento 0439406).

Compulsando os autos, verifica-se que a SEGOV informa que dentre as ações remanescentes do Plano Diretor de TIC 2016-2018 figura a elaboração da Política de Gestão de Riscos de TIC e que a ausência da aludida norma constituiu um dos achados da auditoria no sistema de gestão de governança de TIC realizada em 2018. Por esta razão, apresentou proposta para atendimento à demanda, na forma de minuta de resolução acostada no evento (Processo SEI n. 0001657-51.2019.6.22.8000 – evento 0426547).

Consta, ainda, que a STI promoveu reunião com o Comitê Executivo de TIC (CETIC) para análise da minuta proposta a esta Presidência. Com base nos apontamentos do comitê executivo, foi apresentada uma nova minuta (Processo SEI n. 0001657-51.2019.6.22.8000 – evento 0439406), devidamente assinada pelos membros do CETIC e encaminhada ao Secretário de Tecnologia da Informação e Comunicação para continuidade (Processo SEI n. 0001657-51.2019.6.22.8000 – eventos 0440070 e 0440091).

Instada a se manifestar, a Diretoria-Geral salientou a importância da implantação da política de Gestão de Riscos de Tecnologia da Informação e Comunicação neste Regional e externou concordância com os termos da minuta apresentada (Processo SEI n. 0001657-51.2019.6.22.8000 – evento 0441802).

Como sabido, a Política de Gestão de Riscos tem por objetivo geral estabelecer princípios, diretrizes e responsabilidades para a gestão de riscos, incorporando a visão de riscos à tomada de decisão, em conformidade com as melhores práticas adotadas no setor público.

Já no tocante aos objetivos específicos, a Política de Gestão de Riscos tem a finalidade de promover a identificação de eventos em potencial que afetem a consecução dos objetivos institucionais, bem como o fortalecimento das decisões em resposta aos riscos e o aprimoramento dos controles internos administrativos.

Assim, constatada a relevância da implantação da Política de Gestão de Riscos de Tecnologia da Informação e Comunicação deste Tribunal, submeto a presente minuta de resolução à apreciação dos eminentes pares e voto pela sua aprovação.

EXTRATO DA ATA

Instrução n. 0600238-85.2019.6.22.0000 – Classe 19. Origem: Porto Velho - RO. Relator: Desembargador Sansão Saldanha. Interessado: Tribunal Regional Eleitoral de Rondônia.

Decisão: Resolução aprovada, nos termos do voto do relator, à unanimidade.

Presidência do Senhor Desembargador Sansão Saldanha. Presentes o Senhor Desembargador Kiyochi Mori e os Senhores Juízes Paulo Rogério José, Clênio Amorim Corrêa, Ilisir Bueno Rodrigues e Álvaro Kalix Ferro. Ausente justificadamente o Juiz Flávio Fraga e Silva. Procurador Regional Eleitoral, Luiz Gustavo Mantovani.

72ª Sessão Ordinária do dia 18 de setembro.

Assinado eletronicamente por **SANSAO BATISTA SALDANHA**
14/10/2019 11:50:19

https://pje.tre-ro.jus.br:8443/pje-web/Processo/ConsultaDocumento/listView.seam

19101411501505700000002034335

Publicado Intimação em 17/10/2019.
Disponibilizado no DJ Eletrônico