[redacted]

PORTARIA PRESIDÊNCIA N.º 259/2019 TRE/PRE/ASJES - DISPÕE SOBRE A POLÍTICA DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO DO TRIBUNAL REGIONAL DE MATO GROSSO DO SUL

O Desembargador DIVONCIR SCHREINER MARAN, PRESIDENTE EM EXERCÍCIO DO EGRÉGIO TRIBUNAL REGIONAL ELEITORAL DO ESTADO DO MATO GROSSO DO SUL, no uso das atribuições que lhe são conferidas pelo art. 22, inciso VI, do Regimento Interno do Tribunal (Resolução TRE/MS n.° 170/1997), e

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 autocontrole da gestão;

CONSIDERANDO as normas ABNT NBR ISO 27.005:2011, que fornece as definições de termos relativos à gestão de riscos de segurança da informação; as diretrizes para o processo de gestão de riscos de segurança da informação; e, as 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 COBIT5, por meio dos processos Garantir a Otimização de Riscos (EDM03) e Gerenciar Riscos (APO12);

CONSIDERANDO o contido no Referencial Básico de Governança do TCU, aplicável a Órgãos e Entidades da Administração Pública, especificamente

no que tange à Gestão de Riscos como componente dos mecanismos de governança para o alcance dos objetivos institucionais;

CONSIDERANDO a Resolução CNJ nº 211/2015, art. 12, II, c, que estabelece a necessidade da constituição e manutenção de estrutura para o macroprocesso de segurança da informação, onde está englobada a gestão de riscos de segurança da informação;

RESOLVE:

Art. 1º Instituir a Política de Gestão de Riscos de Segurança da Informação do Tribunal Regional Eleitoral de Mato Grosso do Sul, nos termos desta Portaria.

Art. 2º A Gestão de Riscos de Segurança da Informação constitui processo corporativo contínuo e iterativo, que visa dirigir e controlar as ameaças à segurança da informação, que possam afetar a integridade, a autenticidade, a confidencialidade, a disponibilidade e a irretratabilidade da informação e, consequentemente, o cumprimento dos objetivos estratégicos, táticos e operacionais do Tribunal, oferecendo maior garantia para o sucesso do negócio.

CAPÍTULO I

DAS DEFINIÇÕES

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

1. Comissão de Segurança da Informação (CSI): equipe multidisciplinar oficialmente designada para propor políticas, normas, procedimentos e controles relacionados à Segurança da Informação;

2. Gestão de riscos de Segurança da Informação: atividades coordenadas para dirigir e controlar as ameaças que possam afetar a integridade, a confidencialidade e a disponibilidade da informação;

3. Gestor de riscos: donos de processo e gerentes de projeto com responsabilidade e autoridade para monitorar os riscos, bem como selecionar e implementar uma estratégia adequada de resposta a risco;

4. Processo de gestão de riscos de Segurança da Informação: aplicação sistemática de procedimentos para o estabelecimento do contexto, avaliação, análise crítica, relato e monitoramento dos riscos;

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

CAPÍTULO II

DOS OBJETIVOS DA POLÍTICA DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 4º A Política de Gestão de Riscos de Segurança da Informação tem por objetivo estabelecer princípios, diretrizes e responsabilidades para a gestão de riscos de Segurança da Informação, com vistas a prover a Administração de razoável segurança no cumprimento de sua missão e no alcance dos seus objetivos institucionais, incorporando a visão de riscos à tomada de decisão.

CAPÍTULO III

DOS PRINCÍPIOS DA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 5º A Gestão de Riscos de Segurança da Informação do TRE-MS observará os seguintes princípios:

I - 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 DA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 6º A Gestão de Riscos de Segurança da Informação observará as seguintes diretrizes:

1.Comunicação clara e objetiva, em linguagem comum;

2.Observação das melhores práticas de governança e de gestão de riscos no setor público;

3.Razoabilidade da relação custo-benefício nas ações existentes no Plano de Tratamento de Riscos;

4.Alinhamento e integração com o sistema de governança e com a estratégia institucional.

CAPÍTULO V

DAS RESPONSABILIDADES PELA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 7º São instâncias responsáveis pela Gestão de Riscos de Segurança da Informação do Tribunal:

1.A Diretoria-Geral;

2.A Comissão de Segurança da Informação (CSI);

3.O Gestor de Riscos;

Art. 8ª Compete à Diretoria-Geral:

1.Assegurar a alocação dos recursos necessários à gestão de riscos de Segurança da Informação;

2.Submeter à Presidência do TRE-MS, normativos relativos à Gestão de Riscos de Segurança da Informação e suas alterações, com fundamento em pareceres técnicos submetidos à sua apreciação.

Art. 9ª Compete ao Comissão de Segurança da Informação:

1. Propor a realização de análise de riscos e mapeamento de vulnerabilidades nos ativos;

2. Propor alteração no modelo do Processo de Gestão de Riscos de Segurança da Informação;

3. Apresentar à Diretoria-Geral proposta de revisão e atualização a Política de Gestão de Riscos de Segurança da Informação;

4. Deliberar sobre eventuais riscos que lhe forem apresentados pelos gestores de riscos;

5. Submeter à Diretoria-Geral, eventualmente, os riscos de Segurança da Informação que julgue extrapolarem sua competência.

Art. 10 Compete ao gestor de riscos:

1. Identificar, analisar, avaliar, tratar, monitorar e comunicar os riscos de segurança da informação dos processos de trabalho ou projetos institucionais, sob sua responsabilidade, de acordo com o Processo de Gestão de Riscos de Segurança da Informação instituído.

2. Submeter à Comissão de Segurança da Informação, eventualmente, os riscos de segurança da Informação que julgue extrapolarem sua competência.

CAPÍTULO VI

DAS DISPOSIÇÕES GERAIS

Art. 11 A aplicação desta Política dar-se-á por meio do Processo de Gestão de Riscos de Segurança da Informação, conforme estabelecido no manual em Anexo.

Art. 12 Esta Política deverá ser revisada a cada dois anos, ou a qualquer tempo, quando necessário.

Art. 13 Esta Política de Gestão de Riscos de Segurança da Informação é de uso obrigatório.

Art. 14 Os casos omissos ou excepcionais serão resolvidos pela Diretoria-Geral.

Art. 15 Esta resolução entra em vigor na data de sua assinatura.

Campo Grande (MS), na data da assinatura digital.

Desembargador DIVONCIR SCHREINER MARAN

Presidente em substituição