



**PODER JUDICIÁRIO**  
**TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS**  
**RESOLUÇÃO Nº 15.978**

(24/7/2019)

Dispõe sobre a Política Corporativa de Gestão de Riscos de Tecnologia da Informação e Comunicação, no âmbito do Tribunal Regional Eleitoral de Alagoas.

O TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS, no exercício de suas atribuições legais;

CONSIDERANDO a necessidade de observar o princípio constitucional da eficiência, previsto no art. 37 da Constituição Federal do Brasil;

CONSIDERANDO as orientações do Tribunal de Contas da União (TCU) constantes das 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 gestão;

CONSIDERANDO o teor da Norma ABNT NBR ISO nº 31000:2018, que estabelece princípios e diretrizes para a gestão de riscos;

CONSIDERANDO o que foi registrado no Processo SEI nº 0005319-78.2019.6.02.8000,

**RESOLVE:**

Art. 1º Instituir a Política Corporativa de Gestão de Riscos de Tecnologia da Informação e Comunicação (TIC), no âmbito do Tribunal Regional Eleitoral de Alagoas, que compreende:

I - Objetivos da Política Corporativa de Gestão de Riscos;

II - Princípios da Gestão de Riscos;

III - Diretrizes da Gestão de Riscos;

IV - Responsabilidades da Gestão de Riscos.

Art. 2º Para fins desta Resolução, considera-se:

I - agente responsável: servidor público, ocupante de cargo efetivo do TRE/AL, incumbido de chefiar e gerenciar o grupo de resposta a incidentes de segurança da informação;

II - apetite a riscos: quantidade e tipo de riscos que uma organização está preparada para buscar, reter ou assumir apetite;

III - análise crítica: atividade realizada para determinar a adequação, a suficiência e a eficácia do assunto em questão para atingir os objetivos estabelecidos;

IV - 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;

V - Comitê de Gestão de Tecnologia da Informação e Comunicação (CGTIC): 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;

VI - Comitê de Governança de Tecnologia da Informação e Comunicação (CGovTIC): equipe multidisciplinar, oficialmente designada para deliberar sobre políticas, diretrizes e investimentos em TIC, em conformidade com a norma que o define;

VII - consequência: resultado de um evento que afeta os objetivos estabelecidos;

VIII - contexto: conjunto de fatores internos e externos à organização que, juntamente com os critérios de riscos, definirão o ambiente de gerenciamento dos riscos;

IX - 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;

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

XI - gestão de riscos: atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos;

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

XIII - impacto: grandeza ou dimensão das consequências ou efeitos da ocorrência de um evento;

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

XV - parte interessada: pessoa ou organização que pode afetar, ser afetada ou perceber-se afetada por uma decisão ou atividade;

XVI - 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;

XVII - probabilidade: chance de algo acontecer;

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

XIX - 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;

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

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

XXII - riscos residuais: risco remanescente após o tratamento do risco;

XXIII - 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 CORPORATIVA DE GESTÃO DE RISCOS DE TIC

Art. 3º A política corporativa de que trata esta Resolução tem o objetivo geral de estabelecer princípios, diretrizes e responsabilidades para a gestão de riscos de tecnologia da informação e comunicação, com o intuito de prover razoável segurança no cumprimento da missão institucional do TRE-AL, bem como de incorporar a visão de riscos à tomada de decisões.

Art. 4º A Política Corporativa de Gestão de Riscos de TIC tem os objetivos específicos de 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 DE TIC

Art. 5º A gestão de riscos de tecnologia da informação e comunicação observará os seguintes princípios:

- I - criar e proteger os 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 TIC

Art. 6º A gestão de riscos de tecnologia da informação e comunicação observará as seguintes diretrizes:

- I - comunicação clara e objetiva, em linguagem comum;
- II - observação das melhores práticas de governança e de gestão de riscos no setor público;
- III - razoabilidade da relação custo-benefício nas ações relativas ao tratamento de riscos;
- IV - controle proporcional ao risco.

Art. 7º São elementos estruturais da Gestão de Riscos de TIC:

- I - a Política Corporativa de Gestão de Riscos de TIC;
- II - o processo de Gestão Corporativa de Riscos de TIC;
- III - o Comitê de Governança de TIC;
- IV - o proprietário do risco;
- V - a unidade de assessoramento à governança de TIC ou equivalente;
- VI - a unidade de Controle Interno e Auditoria ou equivalente;
- VII - o monitoramento, a análise crítica e a melhoria contínua dos elementos estruturais.

## CAPÍTULO V

### DAS RESPONSABILIDADES PELA GESTÃO DE RISCOS DE TIC

Art. 8º A Gestão de Riscos de TIC 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 CGTIC;

III - em terceira instância, do CGovTIC;

Parágrafo único. A unidade de Controle Interno e Auditoria ou equivalente deverá atuar como orientadora e promotora do processo de Gestão Corporativa de Riscos de TIC.

Art. 9º Compete ao CGTIC:

I - assegurar a alocação dos recursos necessários à gestão de riscos de TIC;

II - avaliar a adequação, a suficiência e a eficácia da estrutura de Gestão de Riscos de TIC;

III - revisar esta Política Corporativa de Gestão de Riscos de TIC e apresentar proposta de alteração e atualização ao CGovTIC;

IV - operacionalizar, no âmbito das unidades de TIC, a aplicação dos recursos disponibilizados para a gestão de riscos;

V - dirimir eventuais dúvidas dos proprietários de risco, na execução dos processos de Gestão Corporativa de Riscos de TIC;

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

VII - submeter ao CGovTIC, após sua apreciação e manifestação, os riscos considerados extremos e os riscos residuais considerados altos;

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

IX - elaborar o modelo de processo de Gestão Corporativa de Riscos de TIC, e submetê-lo à aprovação do CGovTIC.

Art. 10. Compete ao CGovTIC:

I - deliberar, após apreciação do CGTIC, sobre os riscos considerados extremos e os riscos residuais considerados altos;

II - aprovar o modelo do processo de Gestão Corporativa de Riscos de TIC, elaborado pelo CGTIC.

Art. 11 Compete ao proprietário de risco:

I - gerir os riscos sob sua responsabilidade;

II - reportar ao CGTIC os riscos que eventualmente extrapolem sua competência e capacidade para gerenciamento;

III - encaminhar ao CGTIC os Planos de Gestão de Riscos de TIC de sua responsabilidade.

## CAPÍTULO VI

### DAS DISPOSIÇÕES GERAIS

Art. 12. O Tribunal adotará o modelo de processo de gestão corporativa de riscos estabelecido na norma ABNT NBR ISO nº 31000:2009, sem prejuízo da aplicação de outras normas complementares.

Parágrafo único. A modelagem do processo de Gestão Corporativa de Riscos de TIC deverá ser elaborada e proposta pelo CGTIC em até 180 (cento e oitenta) dias a contar da publicação desta

Resolução.

Art. 13. Esta política deverá ser continuamente revisada, sendo alterada quando houver necessidade.

Art. 14. Os casos omissos ou excepcionais serão resolvidos pelo CGovTIC, após manifestação técnica do CGTIC.

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

Sala de Sessões do Tribunal Regional Eleitoral de Alagoas, em Maceió (AL), aos 24 dias do mês de julho de 2019.

Des. Eleitoral OTÁVIO LEÃO PRAXEDES  
Vice-Presidente e Corregedor no exercício da Presidência

Des. Eleitoral KLEVER RÊGO LOUREIRO

Des. Eleitoral JOSÉ DONATO DE ARAÚJO NETO

Des. Eleitoral CARLOS CAVALCANTI DE ALBUQUERQUE FILHO

Desa. Eleitoral MARIA VALÉRIA LINS CALHEIROS

Des. Eleitoral EDUARDO ANTONIO DE CAMPOS LOPES

Des. Eleitoral HERMANN DE ALMEIDA MELO

Dr<sup>a</sup>. RAQUEL TEIXEIRA MACIEL RODRIGUES  
Procuradora Regional Eleitoral