



**PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 16ª REGIÃO
GABINETE DA PRESIDÊNCIA**



ATO REGULAMENTAR GP/TRT16 Nº 5/2024.

A DESEMBARGADORA PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 16ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO que a gestão de riscos de Tecnologia de Informação e Comunicação (TIC) fornece maior garantia para o alcance dos objetivos institucionais;

CONSIDERANDO a Resolução Administrativa Nº 026/2024 que define a Política de Segurança da Informação e Comunicação e atribui à Presidência do Tribunal a responsabilidade da publicação de atos complementares,

R E S O L V E:

Definir a Política de Gestão de Riscos de Tecnologia da Informação e Comunicação no âmbito do Tribunal Regional do Trabalho da 16ª Região e atualizar o Processo de Gestão de Riscos de TIC, nos termos deste Ato Regulamentar.

CAPÍTULO I

DAS DEFINIÇÕES

Art. 1º Para fins deste Ato Regulamentar, considera-se:

I - Ameaça: ação de origem humana (intencional ou acidental) ou ambiental, que explora uma vulnerabilidade presente num ativo e provoca impactos na organização;

II - Appetite ao risco: é a dimensão e o tipo de risco que uma organização está disposta a aceitar para consecução dos objetivos;

III - Ativo: qualquer recurso que possui valor para a organização e cujo risco precisa ser controlado e gerenciado. Pode ser uma operação, uma atividade, um projeto, um programa, um serviço, um processo, um objetivo estratégico, etc.;

IV - Impacto: consequência sobre os ativos e negócios de uma organização, caso uma ameaça venha a se concretizar. Pode ser tangível (exemplo: perdas financeiras) ou intangíveis (exemplo: perda de credibilidade). Corresponde ao produto "S" (severidade) por "R" (relevância);

V - Probabilidade: é a possibilidade de concretização de uma ameaça. Pode variar de 1-Muito baixa a 5-Muito alta;

VI - PSR: é uma indicação numérica do nível de vulnerabilidade relativo a um risco. Pode variar de 1 a 125 e é o resultado da multiplicação das grandezas: probabilidade, severidade e relevância;

VII - Relevância: grau de importância do ativo para o negócio da organização. Pode variar de 1-Muito baixa a 5-Muito alta;

VIII - Risco: é a combinação da probabilidade de que algum incidente ocorra e sua consequência;

IX - Severidade: medida do grau em que um ativo será afetado, caso uma ameaça venha a se efetivar. Pode variar de 1-Muito baixa a 5-Muito alta.

CAPÍTULO II

DAS DIRETRIZES GERAIS

Art. 2º A Gestão de Riscos de Tecnologia de Informação e Comunicação do Tribunal Regional do Trabalho da 16ª Região obedecerá às seguintes diretrizes:

I - Estabelecer o Processo de Gestão de Riscos de TIC para identificar ameaças, analisar e avaliar riscos de TIC, bem como para definir planos de tratamento destes riscos;

II - Estabelecer as atribuições e responsabilidades relativas à Gestão de Riscos de TIC.

Art. 3º O Processo de Gestão de Riscos de TIC será executado, no mínimo, uma vez ao ano, considerando a Lista de Ativos Críticos definida no âmbito do Plano de Continuidade de Serviços de TIC do Tribunal Regional do Trabalho da 16ª Região, com prazo de 90 (noventa dias) dias para a apresentação do Relatório Geral de Análise de Riscos ao Comitê de Segurança da Informação e Proteção de Dados para apreciação.

§ 1º. As análises de risco deverão ser realizadas por meio do uso de metodologia baseada na norma ISO 27005, que implemente pelo menos os controles CIS versão 8.1 ou superior.

§ 2º. O disposto no caput aplica-se ao responsável pela elaboração do Relatório Geral de Análise de Riscos e aos servidores responsáveis pelo preenchimento dos questionários de análise de riscos relativos aos ativos sob sua responsabilidade.

§ 3º. Ao fim do prazo disposto no caput, os ativos correspondentes a questionários não respondidos serão considerados “não analisados”.

§ 4º. O Relatório Geral de Análise de Riscos deverá indicar o resultado da análise de riscos e recomendar as providências que devem ser adotadas pelos responsáveis pelos ativos. O Plano de Tratamento de Riscos deverá apresentar as demandas de segurança de TIC que serão submetidas ao Processo de Gerenciamento de Demandas de TIC e, eventualmente, convertidas em projetos da SETIC.

§ 5º. As informações relacionadas à implantação e desenvolvimento do processo deverão ser registradas e catalogadas em processo administrativo.

Art. 4º Os níveis de risco a serem considerados no âmbito da Política de Gestão de Riscos de TIC são: muito baixo, baixo, médio, alto e muito alto.

§ 1º. O apetite ao risco de TIC é definido como nível médio, isto é, o Tribunal envidará esforços no sentido de que o PSR dos riscos de TIC seja limitado ao nível médio, conforme descrito no Anexo.

§ 2º. O disposto no §1º subordina-se a relação custo benefício das ações de controle dos riscos, que deve ser sempre positiva.

CAPÍTULO III

DO PROCESSO DE TRABALHO

Art. 5º As atividades executadas no âmbito da Política de Gestão de Riscos de TIC deverão observar os procedimentos descritos no Processo de Gestão de Riscos de TIC;

Parágrafo único. Compete ao Subcomitê de Tecnologia da Informação e Comunicação (STIC) aprovar o processo e suas revisões.

Art. 6º O documento do Processo de Gestão de Riscos de TIC deverá estar disponível no Portal de Governança de TIC do TRT da 16ª Região, e conterá, no mínimo, o desenho dos fluxos, a descrição detalhada das atividades e a definição de papéis e responsabilidades.

Art. 7º O processo de Trabalho será revisto, no mínimo, com periodicidade bienal ou quando precisar ser atualizado.

CAPÍTULO IV

DOS RESPONSÁVEIS E DAS RESPONSABILIDADES

Art. 8º A responsabilidade sobre a execução das atividades previstas no Processo de Gestão de Riscos de TIC caberá aos seguintes responsáveis:

I - Ao Secretário de Tecnologia da Informação e Comunicação caberá a responsabilidade pelo papel de “**Dono do Processo**”;

II - Ao Chefe da Divisão de Infraestrutura e Segurança da Informação caberá a responsabilidade pelo papel de “**Gerente do processo**”.

CAPÍTULO V

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 9º A Política de Gestão de Riscos de TIC aplica-se aos ativos críticos de TIC definidos no âmbito do Plano de Continuidade de Negócio do Tribunal Regional do Trabalho da 16ª Região.

Art. 10º Ficam revogadas as disposições contrárias a este normativo, notadamente a Portaria GP Nº 319/2019, Portaria GP nº 779/2017 e Portaria GP nº 677/2017.

Art. 11º. Os casos omissos serão resolvidos pelo Presidente do Tribunal.

Art. 12º. O presente Ato Regulamentar entra em vigor na data de sua publicação.

Dê-se ciência.

Publique-se no Diário Eletrônico da Justiça do Trabalho e disponibilize-se no Sítio Eletrônico do Egrégio Tribunal.

São Luís/MA, datado e assinado digitalmente.

Desembargadora MÁRCIA ANDREA FARIAS DA SILVA
Presidente do Tribunal Regional do Trabalho da 16ª Região



Av. Senador Vitorino Freire, nº 2001, Areinha, 6º Andar
CEP 65030-015 – São Luís - Maranhão
(98) 2109-9306 / presidencia@trt16.jus.br



Documento assinado eletronicamente por **MÁRCIA ANDREA FARIAS DA SILVA, Presidente**, em 25/03/2024, às 11:56, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site [Autenticar Documentos](#), informando o código verificador **0116032** e o código CRC **A48C4222**.

Referência: Processo nº 000004429/2018

SEI nº 0116032