PORTARIA TRT/GP/DG Nº 182/2024

Define a Política de Gestão de Riscos de Tecnologia de Informação e Comunicações do Tribunal Regional do Trabalho da 24ª Região.

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO, no uso de suas atribuições regimentais,

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

CONSIDERANDO a Resolução Administrativa Nº 32/2024 que define a Política de Segurança da Informação e atribui à Presidência do Tribunal a responsabilidade de publicação de atos complementares;

CONSIDERANDO a aprovação pelo Comitê de Segurança da Informação e Proteção de Dados, em reunião ordinária de 18 de janeiro de 2024, da proposta de minuta para o presente normativo,

R E S O L V E:

DEFINIR a Política de Gestão de Riscos de Tecnologia de Informação e Comunicações no âmbito do Tribunal Regional do Trabalho da 24ª Região, nos termos desta Portaria.

CAPÍTULO I
DAS DEFINIÇÕES

Art. 1º Para fins desta Portaria, 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 - **Apetite 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;

X - **Nuvem**: Infraestrutura de tecnologia para armazenamento de dados, serviços, soluções e sistemas, em ambiente externo ao data center do TRT da 24ª Região;

XI – **On-premisse:** Infraestrutura de tecnologia para armazenamento de dados, serviços, soluções e sistemas, no ambiente do data center do TRT da 24ª Região.

CAPÍTULO II
DAS DIRETRIZES GERAIS

Art. 2° A Gestão de Riscos de Tecnologia de Informação e Comunicações do Tribunal Regional do Trabalho da 24ª Região obedecerá às seguintes diretrizes:

I - estabelecer o Processo "Gerenciar 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. 3° O Processo "Gerenciar Riscos de TIC" será executado, no mínimo, uma vez ao ano, considerando a Lista de Ativos Críticos definida no âmbito da Política de Segurança da Informação do TRT da 24ª Região, com prazo de 45 (quarenta e cinco) dias para a apresentação do Relatório Geral de Análise de Riscos ao Comitê de Segurança da Informação e Proteção de Dados para apreciação.

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

§ 2° 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.

§ 3° Ao fim do prazo disposto no *caput*, os ativos correspondentes a questionários não respondidos serão considerados "não analisados".

§ 4º Os ativos, riscos e vulnerabilidades devem incluir em sua análise as características inerentes ao ambiente de armazenamento, *on-premisse* ou em nuvem conforme o caso em verificação.

§ 5º 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 Gerenciar Demandas" e, eventualmente, convertidas em projetos da SETIC.

§ 6º As informações relacionadas à implantação e desenvolvimento do processo deverão ser registradas e catalogadas em processo administrativo no sistema PROAD.

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 trabalho "Gerenciar Riscos de TIC", disponível no *site* do Portal de Governança de TIC do TRT da 24ª Região, item "Políticas e Processos de Trabalho".

CAPÍTULO IV

DOS RESPONSÁVEIS E DAS RESPONSABILIDADES

Art. 6º A responsabilidade sobre a execução das atividades previstas no processo de trabalho "Gerenciar Riscos de TIC" caberá aos seguintes responsáveis:

I - ao Secretário de Tecnologia da Informação e Comunicações caberá a responsabilidade pelo papel de "**Dono do Processo**";

II - ao Coordenador do Comitê de Segurança da Informação e Proteção de Dados, definido no âmbito da Política de Segurança da Informação, caberá a responsabilidade pelo papel de "**Comitê de Segurança da Informação**";

III - ao Chefe da Divisão de Proteção de Dados e Segurança da Informação caberá a responsabilidade pelo papel de "**Gerente do Processo**".

Art. 7º O gerenciamento dos riscos compete aos integrantes da Equipe de Tratamento e Resposta a Incidente de Segurança Cibernética – ETIR, nos termos da Política de Gestão de Incidentes de Segurança da Informação, relativamente a ações, projetos e iniciativas sob sua responsabilidade, de acordo com o contexto da gestão de riscos de TIC.

CAPÍTULO V

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 8º A Política de Gestão de Riscos de TIC aplica-se aos ativos críticos de TIC definidos no âmbito da **Política de Segurança da Informação** do TRT da 24ª Região.

Art. 9º Ficam revogadas as disposições contrárias a este normativo, notadamente a Portaria TRT/GP/DG Nº 236/2022.

Art. 10. Os casos omissos serão resolvidos pelo Comitê de Segurança da Informação e Proteção de Dados.

Art. 11. Esta Portaria entra em vigor na data de sua publicação.

João Marcelo Balsanelli

Desembargador Presidente

ANEXO

Níveis de Risco

Nível de Risco PSR	**Interpretação**	**Valores Possíveis PSR**
Muito Alto	São riscos inaceitáveis e os gestores dos ativos devem ser orientados para que os eliminem imediatamente.	60, 64, 75, 80, 100, 125
Alto	São riscos inaceitáveis e os gestores dos ativos devem ser orientados para pelo menos controlá-los.	32, 36, 40, 45, 48, 50
Médio	São riscos que podem ser aceitáveis após revisão e confirmação dos gestores dos ativos, contudo a aceitação do risco deve ser feita por meios formais.	18, 20, 24, 25, 27, 30
Baixo	São riscos que podem ser aceitáveis após revisão e confirmação dos gestores dos ativos.	8, 9, 10, 12, 15, 16
Muito Baixo	São riscos aceitáveis e devem ser informados para os gestores dos ativos.	1, 2, 3, 4, 5, 6