PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 19ª REGIÃO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES – SETIC

ATO Nº. 83/GP/TRT 19ª, DE 08 DE AGOSTO DE 2019

Institui as diretrizes para a Gestão de Riscos de TIC no âmbito do Tribunal Regional do Trabalho da 19ª Região.

A DESEMBARGADORA PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA DÉCIMA NONA REGIÃO, no uso de suas atribuições legais e regimentais, tendo em vista o contido no Proad nº 3778/2019, de 17.07.2019,

CONSIDERANDO a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), instituída pela Resolução CNJ n. 211, de 15 de dezembro de 2015;

CONSIDERANDO a publicação pelo Conselho Nacional Justiça de diretrizes gerais para a implantação da Gestão de Segurança da Informação no Poder Judiciário;

CONSIDERANDO as determinações do Acórdão CSJT-A-1453-83.2015.5.90.0000, relativo à Auditoria na Área de Gestão de Tecnologia da Informação;

CONSIDERANDO a Resolução n. 104, de 5 de outubro de 2016, que institui a Política de Gestão de Riscos e de Controles Internos do Tribunal Regional do Trabalho da 19ª Região.

CONSIDERANDO a necessidade de atingir o objetivo estratégico "A-primorar a Gestão de Riscos de TIC" instituído no Plano Estratégico de TIC - PETIC através da adoção de um processo de gestão de riscos de TIC;

CONSIDERANDO a necessidade de orientar a condução da Política de Segurança da Informação (PSI) em vigor no TRT da 19ª Região, visando garantir e incrementar a segurança da informação e das comunicações;

CONSIDERANDO a Resolução n. 166, de 8 de maio de 2019, que dispõe sobre a Política de Governança de Tecnologia da Informação e Comunicação do TRT da 19ª Região; e

CONSIDERANDO as boas práticas de Governança de TIC que visam garantir a disponibilidade e integridade dos sistemas, aplicativos, dados e de documentos digitais do TRT da 19ª Região,

R E S O L V E:

Art. 1º Aprovar o Processo de Gestão de Riscos de Tecnologia da Informação e Comunicação (PGR-TIC) relacionado à infraestrutura, projetos e processos de TIC no âmbito do Tribunal Regional do Trabalho da 19ª Região (TRT19).

Art. 2º O processo de gestão de riscos de TIC deverá observar como metodologia o Plano de Gerenciamento de Riscos do TRT19 (PGR-TRT), instituído pelo Ato TRT 19ª GP n. 86, de 5 de outubro de 2017, e as disposições da Resolução Administrativa n. 104, de 5 de outubro de 2016, que institui a Política de Gestão de Riscos e de Controles Internos do TRT19.

CAPÍTULO I

DAS DEFINIÇÕES

Art. 3º Para fins deste Ato, adotam-se as seguintes definições:

I – contexto – diz respeito à definição dos parâmetros externos e internos e dos critérios de risco a serem levados em consideração no gerenciamento de riscos;

II – controle – medida que está modificando o risco;

III – critérios de risco – termos de referência contra os quais a significância de um risco é avaliada. Os critérios de risco são baseados nos objetivos organizacionais e no contexto externo e contexto interno. Os critérios de risco podem ser derivados de normas, leis, políticas e outros requisitos;

IV – impacto – uma das consequências da ocorrência de um evento. Ocasiona mudança adversa no nível obtido dos objetivos;

V – nível de risco – magnitude de um risco ou combinação de riscos, expressa em termos da combinação dos impactos e de suas probabilidades;

VI – probabilidade **–** chance de algo acontecer;

VII – processo de gestão de riscos de TIC – aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos de TIC;

VIII – processo de trabalho –processos, projetos e ações relacionadas às competências e atribuições das unidades do TRT19;

IX – risco – efeito da incerteza nos objetivos de uma instituição, caracterizado esse efeito por um desvio em relação ao resultado esperado;

X – risco residual – risco remanescente após o tratamento do risco.

CAPÍTULO II

DO PROCESSO DE GESTÃO DE RISCOS DE TIC

Art. 4º O PGR-TIC tem início após a priorização dos processos de trabalho de TIC e segue o processo definido na Política de Gestão de Riscos do TRT – PGR-TRT, aplicado especificamente aos riscos de TIC.

§ Único. Cabe ao Comitê de Governança de TIC priorizar os processos de trabalho, projetos e ações de TIC que devem ter os riscos gerenciados e tratados com prioridade, em face da dimensão dos prejuízos que possam causar, podendo levar em consideração os seguintes critérios de escolha:

I – alinhamento com os objetivos estratégico do PETIC;

II – impacto em caso de incidentes;

III – complexidade do processo de trabalho alvo.

Art. 5º O PGR-TIC é composto por 7 (sete) atividades que interagem de forma cíclica:

I – estabelecimento do contexto específico;

II – identificação dos riscos de TIC;

III – análise dos riscos de TIC;

IV – avaliação dos riscos de TIC;

V – tratamento dos riscos de TIC;

VI – monitoramento e análise crítica;

VII – comunicação e consulta.

Art. 6º Para estabelecer o contexto específico deve-se observar o contexto geral definido na PGR-TRT e ajustar, quando necessário:

I – os fatores internos e externos, adicionando ou excluindo as categorias de eventos que não se aplicam ao processo de trabalho;

II – os critérios de riscos, avaliando e redefinindo de acordo com as necessidades específicas, âmbito e escopo de atuação;

III – a escala de probabilidade, redefinindo o número de ocorrências para cada descritor;

IV – a escala de impacto, redefinindo o custo e o prazo e;

V – a matriz de classificação de riscos.

§ 1º O contexto específico deve estabelecer os objetivos, escopo e limites da avaliação de riscos a ser realizada com a identificação das partes interessadas. As exclusões do escopo devem também ser definidas e justificadas.

§ 2º A definição de contexto e a matriz RACI (Responsável, Aprovador, Consultado, Informado) são elaboradas pela equipe da SETIC, validadas pelo Comitê Gestor de TIC - CGESTIC e aprovadas pelo Comitê de Governança de TIC - CGTIC.

Art. 7º A identificação dos riscos tem como propósito conhecer quais riscos podem influenciar o cumprimento dos objetivos da Instituição.

§ Único. Para auxiliar a identificação de riscos, podem ser utilizadas técnicas e ferramentas como brainstorming, questionários, entrevistas, checklist, análise SWOT (forças, fraquezas, oportunidades e ameaças), análise de dados históricos, análise de premissas, opiniões especializadas, necessidades das partes interessadas e diagramas de causa e efeito.

Art. 8º A análise dos riscos tem como propósito definir o nível de risco, a partir dos níveis de probabilidade e de impacto.

§ 1º Para definir o nível de impacto, deve-se avaliar quais dimensões (custo, prazo, escopo e qualidade) do objetivo do processo de trabalho serão influenciadas direta ou indiretamente.

§ 2º Para que o nível do risco seja definido, os níveis de probabilidade e de impacto são relacionados.

Art. 9º A avaliação de riscos utiliza os resultados da análise de riscos como subsídio para a tomada de decisões sobre quais riscos necessitam ser tratados e quais terão prioridade no tratamento.

§ 1º Deve-se confrontar os níveis de riscos com os controles existentes a fim de testar a eficácia e a eficiência destes.

§ 2º Existindo mais de um controle, deve-se calcular o risco residual de cada um e submetê-los à média aritmética simples.

§ 3º Com base nas diretrizes para priorização do tratamento de riscos definidas na PGR-TRT e no risco residual encontrado na avaliação de riscos obtém-se a recomendação para tratamento do risco.

Art. 10 O tratamento de riscos tem como propósito determinar a resposta mais adequada para modificar a probabilidade ou o impacto de um risco. Essa resposta conta com as seguintes opções:

I – **evitar**: o objetivo dessa resposta é descontinuar as atividades que geram o risco;

II – **transferir**: o objetivo dessa resposta é compartilhar ou transferir uma parte do risco a terceiros sendo que nem todos os riscos são totalmente transferíveis;

III – **mitigar**: o objetivo dessa resposta é reduzir a probabilidade, o impacto, ou ambos;

IV – **aceitar**: o objetivo dessa resposta é avaliar se os demais tipos de respostas ao risco são viáveis.

§ 1º O tipo de resposta a ser utilizado deverá ser aplicado dentro do intervalo de tempo definido pelo Secretário da Unidade, ou cargo equivalente.

§ 2º Nesta etapa deve ser construído o Plano de Tratamento de Riscos (PTR).

§ 3º O Comitê Gestor de TIC deverá avaliar o PTR confirmando o impacto dos riscos que serão aceitos e encaminhando para tratamentos os que devem ser evitados, transferidos ou mitigados.

§ 4º O PTR deve ser aprovado pelo Comitê de Governança de TIC.

Art. 11 O monitoramento e análise crítica tem como propósito monitorar regularmente e sugerir melhorias durante todas as atividades do Processo de Gestão de Riscos de TIC.

Art. 12 A comunicação e consulta tem como propósito auxiliar todas as atividades do Processo de Gestão de Riscos, de forma a permitir a comunicação eficiente, bem como a consulta às informações pertinentes ao exercício de cada uma delas.

CAPÍTULO III

DAS DISPOSIÇÕES FINAIS

Art. 13 Este processo deverá ser revisto sempre que necessário e, se for o caso, encaminhada proposta à Presidência, após aprovação pelo do Comitê de Governança de TIC, a fim de implementar eventuais melhorias identificadas, executando-se as ações corretivas ou preventivas aprovadas, assegurando que as melhorias atinjam os objetivos pretendidos.

Art. 14 O presente Ato entra em vigor a partir da data de sua publicação.

Art. 15 Revogam-se as disposições em contrário.

Dê-se ciência, cumpra-se e

Publique-se.

Original assinado
ANNE HELENA FISCHER INIJOSA
Desembargadora Presidente

Publicada no D.E.J.T e no BI nº 08, ambos de 09/08/2019.