Poder Judiciário
Justiça do Trabalho
Tribunal Regional do Trabalho da 13ª Região

ATO TRT SGP N.º 71, DE 18 DE JUNHO DE 2020

Institui o Processo de Gestão de Risco de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 13ª Região.

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA DÉCIMA TERCEIRA REGIÃO, no uso de suas atribuições legais, regimentais e considerando o protocolo 000-4699/2020,

considerando as diretrizes da Política de Segurança da Informação e Comunicações da instituição;

considerando a necessidade de manter a continuidade dos serviços essenciais que a instituição presta à sociedade;

considerando a legislação federal, assim como resoluções, normas, recomendações e boas práticas publicadas pelo CNJ, CSJT, TCU e ABNT relacionadas à Segurança da Informação,

R E S O L V E

Art. 1º Estabelecer o Processo de Gestão de Riscos de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 13ª Região, conforme descrição, papéis e responsabilidades definidas no Anexo I.

Art. 2º O presente Ato entra em vigor a partir da data de sua publicação.

Art. 3º Revogam-se as disposições em contrário, especialmente o ATO TRT GP Nº 458/2016.

Dê-se ciência.
Publique-se no DA_e.

WOLNEY DE MACEDO CORDEIRO:103147770
Assinado de forma digital por WOLNEY DE MACEDO CORDEIRO:103147770
Dados: 2020.06.18 15:54:28 -03'00'

WOLNEY DE MACEDO CORDEIRO
Desembargador Presidente

Tribunal Regional do Trabalho
13ª Região | Paraíba

MANUAL DO PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Seção de Segurança da Informação

João Pessoa – 2020
Versão 2.0

Tribunal Regional do Trabalho da 13ª Região

Desembargador Presidente

Wolney de Macedo Cordeiro

Comitê Gestor de Segurança da Informação

Lindinaldo Silva Marinho (Presidente)

Antônio Fragoso Cavalcante Neto

Francisco Hirllen de Oliveira Mendonça

Isêlma Maria de Souza Rodrigues

Rodrigo Cartaxo Marques Duarte

Rodrigo Mafra

Seção de Segurança da Informação

Rodrigo Mafra (Chefe)

Manuel Rodrigues Vieira da Silva

SUMÁRIO

Sumário

1. Objetivo

Definir o Processo de Gestão de Riscos de Segurança da Informação.

2. Propósito do processo

Este processo tem como propósito definir a gestão de riscos de Segurança da Informação no âmbito do Tribunal Regional do Trabalho – 13ª Região, garantindo que os riscos sejam conhecidos, monitorados e tratados, promovendo a manutenção de um nível de risco aceitável.

3. Escopo

O escopo do processo é o mesmo do Sistema de Gestão de Segurança da Informação – SGSI, definido pelo Comitê Gestor de Segurança da Informação - CGSI.

4. Definições e abreviações

Para efeitos deste manual, aplicam-se as definições da Política de Segurança da Informação e Comunicações, além das seguintes:

- **Risco:** fator ou evento incerto que pode causar impactos negativos, dificultando ou impossibilitando o cumprimento dos objetivos; ou positivos, com potencial de agregar valores;
- **Risco de Segurança da Informação:** probabilidade de impacto negativo nos objetivos da organização caso as suas informações não estejam protegidas adequadamente;
- **Gestão de riscos:** conjunto de atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos, contribuindo para a redução da materialização de eventos que impactem negativamente seus objetivos;
- **Gestão de riscos de Segurança da Informação:** gestão de riscos aplicada ao escopo da Segurança da Informação;
- **Tolerância ao risco ou apetite de risco**: é a quantidade de risco que a instituição está propensa a aceitar para alcançar seus objetivos, podendo definir ainda níveis de desvio aceitáveis no desempenho de suas atividades;
- **Controle:** qualquer medida que visa minimizar um risco ou grupo de riscos;
- **Nível ou índice de risco**: magnitude de um risco ou combinação de riscos;
- **Identificação de riscos:** etapa da gestão de riscos que visa localizar, listar e caracterizar os riscos;

- **Análise de riscos:** etapa da gestão de riscos que visa compreender a natureza dos riscos e determinar o nível de risco. A análise de riscos fornece a base para a avaliação de riscos e para as decisões sobre o tratamento de riscos. A análise de riscos inclui a estimativa de riscos;
- **Avaliação de riscos:** etapa da gestão de riscos onde são definidos quais os riscos identificados na análise serão aceitos ou tratados, bem como priorizar o tratamento dos mesmos;
- **Tratamento de riscos:** etapa da gestão de riscos onde são implementadas ações e controles visando reduzir o nível de risco para um patamar aceitável;
- **Relatório de Análise de Riscos (RAR):** apresenta, de forma consolidada, o resultado da análise de riscos;
- **Relatório Operacional de Riscos (ROR):** apresenta o detalhamento das ações e controles que devem ser implementados para eliminar ou mitigar os riscos;
- **Plano de Tratamento de Riscos (PTR):** descreve as ações de tratamento de riscos, identificando os responsáveis, com o objetivo de reduzir os riscos a níveis aceitáveis.

5. Benefícios esperados

A implementação do Processo de Gestão de Riscos de Segurança da Informação no TRT da 13ª Região promoverá os seguintes benefícios:

- Manutenção de níveis aceitáveis de riscos de Segurança da Informação;
- Aderência à Política de Segurança da Informação e Comunicações (POSIC) da instituição, promovendo a confidencialidade, disponibilidade e integridade das informações.

6. Interfaces com demais processos

- **Processo de Gestão de Vulnerabilidades de TIC**: o tratamento das vulnerabilidades influenciará na diminuição dos riscos de Segurança da Informação.

7. Entradas e saídas

As principais entradas e saídas do Processo de Gestão de Riscos de Segurança da Informação são:

7.1 Entradas

- Escopo do SGSI definido pelo CGSI;
- Inventário de Ativos.

7.2 Saídas

- Relatório de Análise de Riscos – RAR;
- Relatório Operacional de Riscos – ROR;
- Plano de Tratamento de Riscos;
- Relatório de Execução do Plano de Tratamento de Riscos – RE.

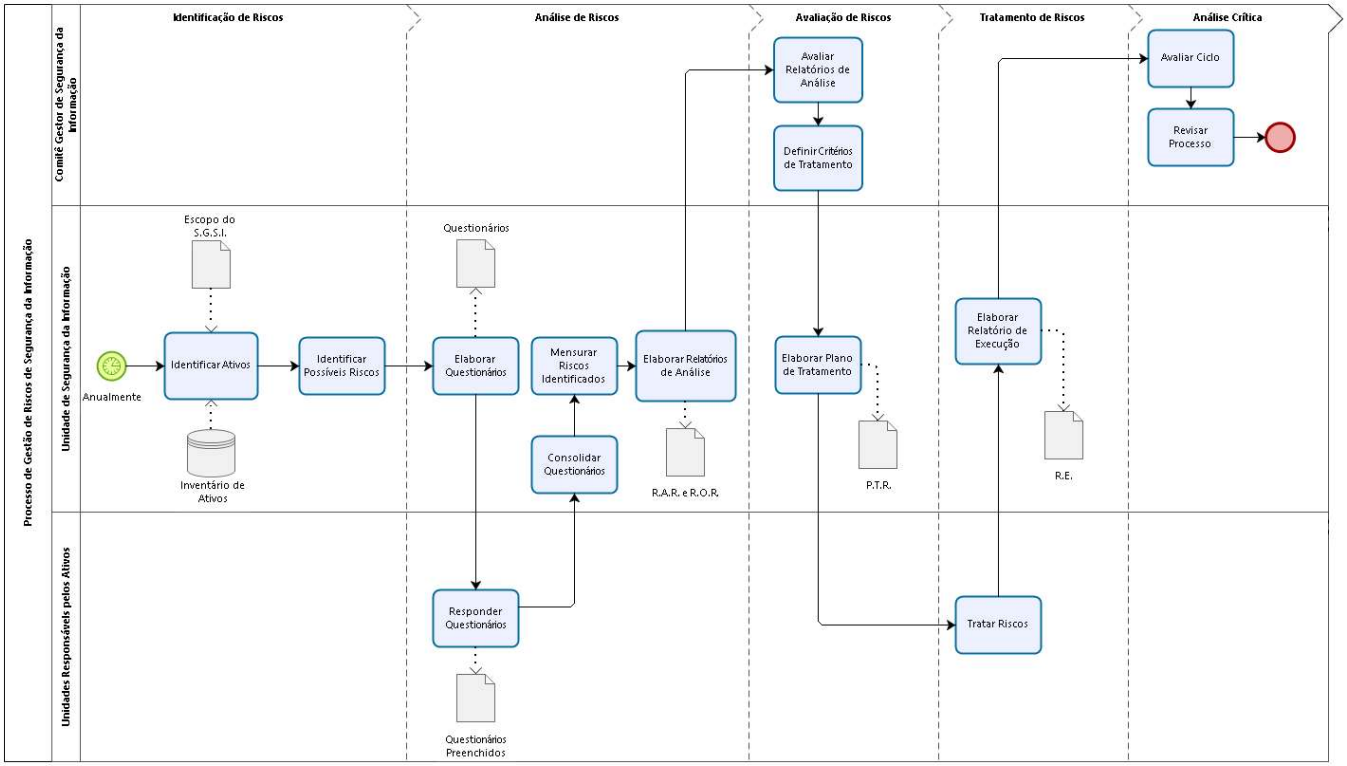
8. Papéis e responsabilidades

Abaixo estão definidos os papéis, seus executores e suas responsabilidades:

PAPEL	DESCRIÇÃO	RESPONSABILIDADES
Comitê Gestor de Segurança da Informação	Comitê multidisciplinar formado por magistrados e servidores, de assessoramento da Administração na área de Segurança da Informação.	Analisar e manifestar-se sobre o processo de Gestão de Riscos de Segurança da Informação, apoiando a Presidência na avaliação do processo.
Unidade de Segurança da Informação (SI)	Unidade responsável pelo macroprocesso de Segurança da Informação e pelo Processo de Gestão de Riscos de Segurança da Informação	Efetuar a análise de riscos de segurança da informação.
		Elaborar Relatório de Análise de Riscos, Relatório Operacional de Risco e Relatório de Execução de Plano de Tratamento de Riscos.
		Assessorar o Comitê Gestor de Segurança da Informação na análise e na tomada de decisões a respeito do Processo de Gestão de Riscos de Segurança da Informação.
		Informar os riscos detectados e recomendar o tratamento dos mesmos.
		Gerenciar o Processo de Gestão de Riscos de Segurança da Informação e manter a documentação relacionada atualizada.
Unidades Responsáveis Pelos Ativos	Compreende as unidades responsáveis pelos ativos que fazem parte do escopo do Processo de Gestão de Riscos de Segurança da Informação.	Tratar os riscos dos ativos sob sua responsabilidade.
		Documentar o tratamento dos riscos.
		Justificar os riscos não tratados.

9. O Processo de Gestão de Riscos de Segurança da Informação

O Processo de Gestão de Riscos de Segurança da Informação é mostrado no diagrama abaixo e em seguida são descritas as atividades do processo.



Identificar Ativos		
Descrição	Identifica os ativos e seus componentes que façam parte do escopo do SGSI, bem como os seus responsáveis.	
Considerações Importantes	N/A	
Papéis	Unidade de SI.	
Entradas	Escopo do SGSI, Inventário de Ativos.	
Saídas	Rol de ativos, componentes e responsáveis.	
Atividades	**Consultar Inventário de Ativos**	Obtém informações dos ativos e seus componentes que façam parte do escopo do SGSI, consultando o Inventário de Ativos.
	Registro Ativos do Escopo	Armazenar adequadamente o rol de ativos e seus componentes que façam parte do escopo do SGSI, bem como os seus responsáveis.
Modelos	N/A	

Identificar Possíveis Riscos		
Descrição	Para cada ativo e seus componentes, identifica os possíveis riscos associados.	
Considerações importantes	N/A	
Papéis	Unidade de SI.	
Entradas	Rol de ativos, componentes e responsáveis.	
Saídas	Rol de possíveis riscos e controles associados para cada ativo e seus componentes.	
Atividades	**Consultar Base de Conhecimento**	Consultar base de conhecimento para levantar os possíveis riscos de cada ativo e seus componentes, bem como os possíveis controles que possam minimizar os riscos.
	Registrar Possíveis Riscos	Armazenar adequadamente os possíveis riscos de cada ativo e seus componentes e seus controles associados.
Modelos	N/A	

Elaborar Questionários		
Descrição	Elaborar os questionários para identificação dos riscos dos ativos e seus componentes.	
Considerações importantes	Caso seja possível, será realizada coleta automática de informações dos riscos dos ativos e seus componentes.	
Papéis	Unidade de SI.	
Entradas	Rol de ativos, componentes e responsáveis; rol de possíveis riscos e controles associados para cada ativo e seus componentes.	
Saídas	Questionário de identificação de riscos.	
Atividades	**Elaborar Questionário**	Para cada ativo e componente, consolidar as entradas acima para compor questionário visando identificar quais os controles foram implementados ou não.
	Coletar Informações Automaticamente	Caso possível, fazer coleta automática de informações de riscos, completando o que for possível nos questionários de identificação de riscos.
	Disponibilizar Questionários	Disponibilizar os questionários de identificação de riscos para os responsáveis pelos ativos e definir prazo para resposta e devolução dos mesmos.
Modelos	N/A	

Responder Questionários		
Descrição	Responder questionário de identificação de riscos.	
Considerações importantes	N/A	
Papéis	Unidade Responsável Pelo Ativo	
Entradas	Questionário de identificação de riscos para cada ativo de sua responsabilidade.	
Saídas	Questionário de identificação de riscos respondido para cada ativo do escopo do processo.	
Atividades	**Verificar Controles**	Para cada ativo e seus componentes, verificar quais os controles estão implementados ou não.
	Preencher Questionário	Com base nas informações obtidas na atividade anterior, preencher o questionário de identificação de riscos.
	Devolver Questionário Respondidos	Devolver para a Unidade de SI os questionários respondidos no prazo estabelecido.
Modelos	N/A	

Consolidar Questionários		
Descrição	Consolidar os questionários de identificação de riscos respondidos.	
Considerações importantes	N/A	
Papéis	Unidade de SI.	
Entradas	Questionários de identificação de riscos respondidos.	
Saídas	Consolidação de todos os questionários de identificação de riscos respondidos.	
Atividades	**Registrar Questionários**	Armazenar adequadamente os questionários de identificação de riscos respondidos.
Modelos	N/A	

Mensurar Riscos Identificados		
Descrição	Com base nos questionários de identificação de riscos respondidos, calcular o risco para cada ativo, componente e do escopo.	
Considerações importantes	O Índice de Risco será calculado de acordo com a metodologia adotada pela ferramenta que auxilia o processo e será dado em percentual.	
Papéis	Unidade de SI.	
Entradas	Questionários de identificação de riscos consolidados.	
Saídas	Índices de Risco de cada ativo, componente e do escopo do processo.	
Atividades	**Calcular Índices de Risco**	Para cada ativo, componente e o escopo inteiro, calcular o Índice de Risco.
	Registrar Índices de Risco	Armazenar adequadamente os Índices de Risco calculados.
Modelos	N/A	

Elaborar Relatórios de Análise		
Descrição	Elaborar Relatório de Análise de Riscos e Relatório Operacional de Riscos.	
Considerações importantes	Os relatórios seguirão modelo da ferramenta que auxilia o processo.	
Papéis	Unidade de SI.	
Entradas	Questionários de identificação de riscos consolidados e Índices de Risco de cada ativo, componente e do escopo do processo.	
Saídas	Relatório de Análise de Riscos e Relatório Operacional de Riscos.	
Atividades	**Confeccionar Relatórios**	Com base nas informações obtidas nas entradas acima, fazer o Relatório de Análise de Riscos e o Relatório Operacional de Riscos.
	Registrar Relatórios	Armazenar os relatórios de maneira adequada.
	Encaminhar Relatórios	Encaminhar os relatórios acima para apreciação do Comitê Gestor de Segurança da Informação.
Modelos	N/A	

Avaliar Relatórios de Análise		
Descrição	Avaliar o Relatório de Análise de Riscos e o Relatório Operacional de Riscos durante reunião do Comitê Gestor de Segurança da Informação.	
Considerações importantes	N/A	
Papéis	Comitê Gestor de Segurança da Informação.	
Entradas	Relatório de Análise de Riscos e o Relatório Operacional de Riscos.	
Saídas	Ciência por parte do CGSI dos riscos do SGSI.	
Atividades	**Apresentação dos Relatórios**	Apresentar o Relatório de Análise de Riscos e o Relatório Operacional de Riscos.
	Discutir Relatórios	Discutir os resultados apresentados nos relatórios.
Modelos	N/A	

Definir Critérios de Tratamento		
Descrição	Definir os critérios de tratamento de riscos que selecionarão os controles que deverão ser implementados.	
Considerações importantes	Os controles que não forem abrangidos pelos critérios de tratamento de riscos terão os riscos da sua não implementação aceitos.	
Papéis	Comitê Gestor de Segurança da Informação.	
Entradas	Relatório de Análise de Riscos e o Relatório Operacional de Riscos.	
Saídas	Critérios de tratamento de riscos.	
Atividades	**Discutir o que Tratar**	Debater sobre quais riscos a instituição deve tratar.
	Estabelecer Critério	Definir o que tratar. Por exemplo: Riscos Muito Altos.
Modelos	N/A	

Elaborar Plano de Tratamento		
Descrição	Elaborar Plano de Tratamento de Riscos de acordo com os critérios estabelecidos pelo CGSI.	
Considerações importantes	N/A	
Papéis	Unidade de SI.	
Entradas	Relatório Operacional de Riscos e critérios de tratamento de riscos.	
Saídas	Plano de Tratamento de Riscos.	
Atividades	**Elaborar Plano**	Considerando os critérios de tratamento de riscos estabelecidos pelo CGSI, elaborar o Plano de Tratamento de Riscos baseado no subconjunto do ROR.
	Disponibilizar Plano	Disponibilizar Plano de Tratamento de Riscos para as unidades responsáveis pelos ativos e estabelecer prazo.
Modelos	N/A	

Tratar Riscos		
Descrição	Tratar os riscos dos ativos sob a sua responsabilidade.	
Considerações importantes	N/A	
Papéis	Unidade Responsável pelo Ativo.	
Entradas	Plano de Tratamento de Riscos.	
Saídas	Plano de Tratamento de Riscos atualizado.	
Atividades	**Implementar Controle**	Quando viável, implementar os controles propostos no Plano de Tratamento de Risco.
	Documentar Implantação	Armazenar adequadamente os procedimentos adotados na implantação dos controles propostos no Plano de Tratamento de Riscos. Indicar no Plano de Tratamento de Riscos que o controle foi implementado.
	Justificar não Implementação	Quando não for viável a implantação de um controle, registrar no Plano de Tratamento de Riscos a justificativa.
	Devolver o PTR atualizado	Devolver o PTR atualizado para a Unidade de Segurança da Informação.
Modelos	N/A	

Elaborar Relatório de Execução		
Descrição	Elaborar Relatório de Execução do Plano de Tratamento de Riscos.	
Considerações importantes	N/A	
Papéis	Unidade de SI.	
Entradas	Relatório de Análise de Riscos, Relatório Operacional de Riscos, Plano de Tratamento de Riscos, Critérios de Tratamento de Risco.	
Saídas	Relatório de Execução de Plano de Tratamento de Riscos.	
Atividades	**Calcular Indicadores**	Calcula os indicadores do processo, de acordo com item 10.
	Elaborar Relatório	Elaborar relatório resumido do ciclo do processo, indicando os fatos relevantes, os indicadores, evolução do risco e sugestões de melhoria.
Modelos	N/A	

Avaliar Ciclo		
Descrição	Avaliar Ciclo do Processo de Gestão de Riscos.	
Considerações importantes	N/A	
Papéis	Comitê Gestor de Segurança da Informação.	
Entradas	Relatório de Execução de Plano de Tratamento de Riscos.	
Saídas	Relatório de Execução de Plano de Tratamento de Riscos revisado.	
Atividades	**Discutir Relatório**	Discutir resultados apresentados no Relatório de Execução do Plano de Tratamento de Riscos.
	Definir melhorias	Definir melhorias para o Processo de Gestão de Riscos de Segurança da Informação.
Modelos	N/A	

Revisar Processo		
Descrição	Revisar o Processo de Gestão de Riscos de Segurança da Informação.	
Considerações importantes	N/A	
Papéis	Comitê Gestor de Segurança da Informação.	
Entradas	Relatório de Execução de Plano de Tratamento de Riscos revisado.	
Saídas	Processo de Gestão de Riscos de Segurança da Informação revisado.	
Atividades	**Fazer Análise Crítica do Processo**	Avaliar se o processo está atendendo as necessidades da instituição.
	Definir Melhorias	Definir melhorias a serem adotadas no processo.
Modelos	N/A	

10. Indicadores de desempenho

10.1 Nível de Risco de Segurança da Informação

Indicador 1	
Objetivo	Avaliar o Nível de Risco de Segurança da Informação da instituição.
Indicador	Percentual de Risco de Segurança da Informação após o tratamento dos riscos.
Responsável pela medição	Unidade de SI.
Período de Medição	Anual.

10.2 Eficiência do Processo

Indicador 2	
Objetivo	Avaliar a eficiência do Processo de Gestão de Riscos de Segurança da Informação
Indicador	(Nível de Risco de Segurança da Informação antes do tratamento menos o Nível de Risco de Segurança da Informação após o tratamento) / Nível de Risco de Segurança da Informação antes do tratamento.
Responsável pela medição	Unidade de SI.
Período de Medição	Anual.

10.3 Eficácia do Processo

Indicador 3	
Objetivo	Avaliar a eficácia do Processo de Gestão de Riscos de Segurança da Informação
Indicador	1 – Se o Nível de Risco de Segurança da Informação após o tratamento estiver dentro da meta de risco aceitável (apetite de risco) da instituição. 0 – Caso contrário.
Responsável pela medição	Unidade de SI.
Período de Medição	Anual.

11. Anexos

11.1 Anexo I – Nível de Risco de Segurança da Informação

Nível de criticidade	Valor
Muito Alto	Acima de 80% (oitenta por cento)
Alto	Maior que 60% (sessenta por cento) e até 80% (oitenta por cento)
Médio	Maior que 40% (quarenta por cento) e até 60% (sessenta por cento)
Baixo	Maior que 20% (vinte por cento) e até 40% (quarenta por cento)
Muito Baixo	Até 20% (vinte por cento)