REGINA GLAUCIA CAVALCANTE NEPOMUCENO

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO TRT7.GP Nº 114, DE 10 DE JUNHO DE 2022

Institui a Norma Complementar de Gestão de Vulnerabilidades de Tecnologia da Informação no âmbito do Tribunal Regional do Trabalho da 7ª Região (TRT7).

A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO o Manual de Referência para Proteção de Infraestruturas Críticas de Tecnologia da Informação e Comunicação (TIC) do Poder Judiciário, estabelecido no Anexo IV da Portaria do Conselho Nacional de Justiça (CNJ) nº 162, de 10 de junho de 2021, que estabelece a necessidade de gerenciamento contínuo de vulnerabilidades,

RESOLVE:

Art. 1º Estabelecer o Processo de Gestão de Vulnerabilidades de TIC no âmbito do Tribunal Regional do Trabalho da 7ª Região, conforme descrição, papéis e responsabilidades definidas no Anexo I.

Art. 2º Este ato entra em vigor na data de sua publicação.

Fortaleza, 10 de junho de 2022.

Regina Gláucia Cavalcante Nepomuceno
Presidente do Tribunal

Documento 4 do PROAD 2546/2022. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2022.ZRLW.LMFP: https://proad.trt7.jus.br/proad/pages/consultadocumento.xhtml

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ANEXO I

Sumário

1. Objetivo 2

2. Propósito do processo 2

3. Escopo 2

4. Definições e abreviações 2

5. Benefícios esperados 2

6. Interfaces com demais processos 3

7. Entradas e saídas 3
7.1 Entradas 3
7.2 Saídas 3

8. Papéis e responsabilidades 3

9. O Processo de Gestão de Vulnerabilidades de TIC 4
9.1 Desenho do processo 4
9.2 Identificar Vulnerabilidade 5
9.3 Registrar demanda 6
9.4 Avaliar demanda 7
9.5 Tratar vulnerabilidade 8
9.6 Fechar Demanda 10
9.7 Elaborar relatório 10

10. Indicadores de desempenho 11

11. Anexos 12
11.1 Anexo I – Tabela de Classificação de Vulnerabilidades 12

1. Objetivo

Definir o Processo de Gestão de Vulnerabilidades de TIC.

2. Propósito do processo

Este processo tem como propósito definir a gestão de vulnerabilidades de TIC no âmbito do Tribunal Regional do Trabalho da 7ª Região, garantindo que as mesmas sejam conhecidas, monitoradas e tratadas.

3. Escopo

O escopo do processo compreende os serviços essenciais de TIC oferecidos pela Secretaria de Tecnologia da Informação e Comunicação (SETIC) do TRT da 7ª Região, sobretudo os que suportam a atividade jurisdicional.

4. Definições e abreviações

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

Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de Segurança da Informação;

Gestão de Vulnerabilidades de TIC: processo de gestão que visa conhecer, monitorar e tratar vulnerabilidades que afetem os ativos de TIC, minimizando o risco de que as mesmas sejam exploradas;

Serviço de TIC: serviço baseado no uso da Tecnologia da Informação, provido a um ou mais clientes para apoiar os processos de negócio da instituição.

5. Benefícios esperados

A implementação do Processo de Gestão de Vulnerabilidades de TIC no TRT da 7ª Região promoverá os seguintes benefícios:

- Redução dos riscos de incidentes de segurança da informação, que utilizem exploração de vulnerabilidades como técnica de ataque;
- Aderência à Política de Segurança da Informação e Comunicações da instituição, promovendo a confidencialidade, disponibilidade e integridade das informações.

6. Interfaces com demais processos

Processo de Gestão de Riscos de Segurança da Informação: 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 Vulnerabilidades de TIC são:

7.1 Entradas

- Alerta de vulnerabilidades oriundas de fontes externas (listas de discussão, sites especializados, etc);
- Resultado de varredura de vulnerabilidades;
- Inventário de Ativos.

7.2 Saídas

- Inventário de Ativos atualizado;
- Base de Conhecimento atualizada;
- Relatório anual do processo.

8. Papéis e responsabilidades

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

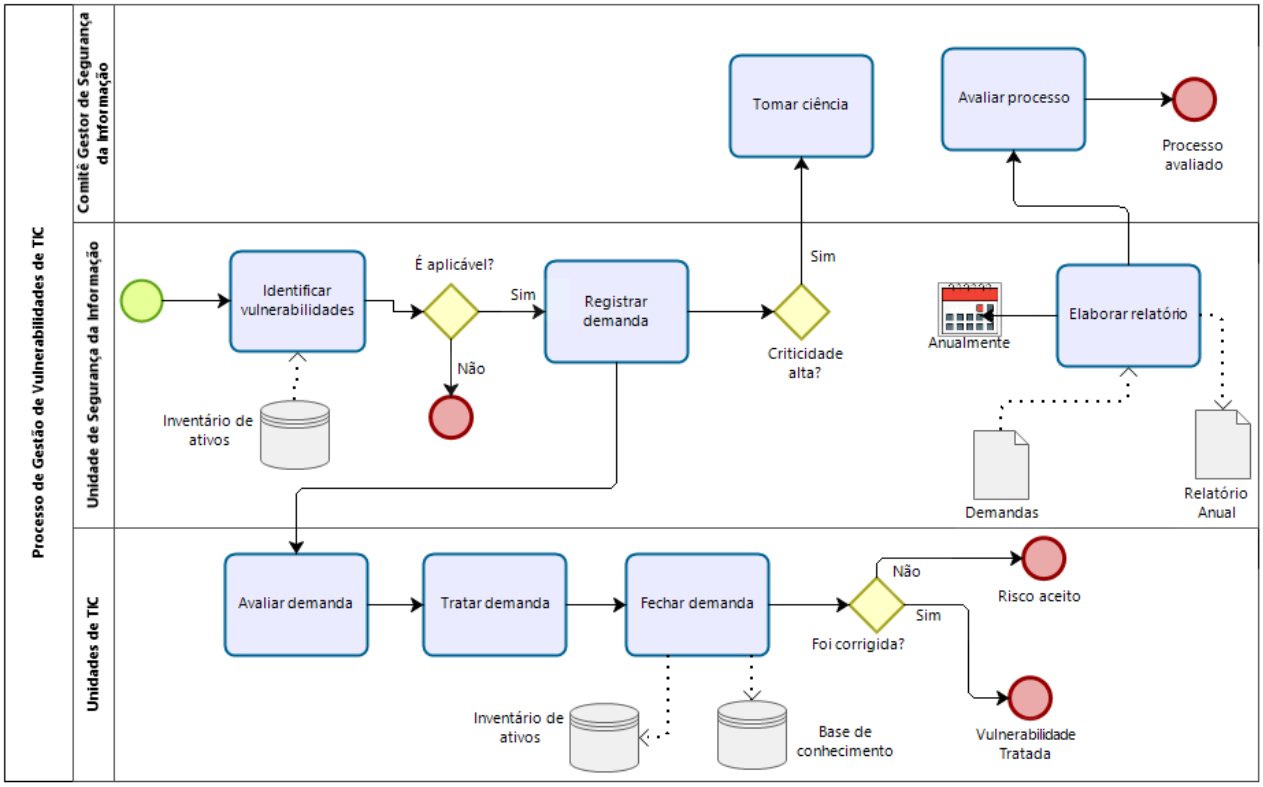
PAPEL	RESPONSABILIDADES

Comitê Gestor de Segurança da Informação (CGSI)	Analisar e manifestar-se sobre o processo de Gestão de Vulnerabilidades de TIC, apoiando a Presidência na avaliação do processo.
Unidade de Segurança da Informação (SI)	Monitorar serviços de alerta de vulnerabilidades e executar varreduras de vulnerabilidades.
	Fazer Relatório Anual de Tratamento de Vulnerabilidades.
	Assessorar o CGSI na análise e na tomada de decisões a respeito do Processo de Gestão de Vulnerabilidades de TIC.
	Abrir demanda para tratamento de vulnerabilidades detectadas ou conhecidas e encaminhá-las à área responsável pelo tratamento.
	Gerenciar o Processo de Gestão de Vulnerabilidades de TIC e manter a documentação relacionada atualizada.
Unidades Técnicas de TIC	Detalhar e incluir as demandas recebidas no planejamento de execução, considerando a criticidade definida.
	Tratar as vulnerabilidades dos ativos sob sua responsabilidade.
	Documentar o tratamento ou não das vulnerabilidades.
	Atualizar o Inventário de Ativos.

9. O Processo de Gestão de Vulnerabilidades de TIC

9.1 Desenho do processo

O Processo de Gestão de Vulnerabilidades de TIC é mostrado no diagrama abaixo.



9.2 Identificar Vulnerabilidade

Identificar vulnerabilidades	
Descrição	Identificar vulnerabilidades que afetem os ativos de TIC da instituição.
Papéis	Unidade de segurança da informação.
Entradas	Inventário de Ativos; E-mail/notificação alertando vulnerabilidade; Resultado de varredura ou Qualquer outra fonte de informações sobre vulnerabilidades.
Saídas	Vulnerabilidades detectadas e ainda não tratadas.

Atividades	Realizar cadastro em serviços de alerta de vulnerabilidades	Cadastrar e-mail da unidade de Segurança da Informação nos principais serviços de alerta de vulnerabilidades.
	Obter informações sobre vulnerabilidades	Obter informações sobre vulnerabilidades através de listas de discussão, varredura de vulnerabilidades ou qualquer outra fonte de informações sobre vulnerabilidades.
	Verificar pertinência	Para cada vulnerabilidade conhecida, verificar se a mesma afeta ativos de TIC da instituição, consultando o Inventário de Ativos e se a mesma ainda não foi tratada.
	Classificar vulnerabilidades	Classificar cada vulnerabilidade pertinente de acordo com a pontuação atribuída preferencialmente pela ferramenta utilizada, pelas fontes especializadas ou, ainda, caso inexistentes, utilizar a Tabela de Classificação de Vulnerabilidades em anexo.
Modelo	Tabela de Classificação de Vulnerabilidades (Anexo I).	

9.3 Registrar demanda

Registrar demanda	
Descrição	Registrar demanda de tratamento de cada vulnerabilidade que afete ativos de TIC da instituição e que façam parte do escopo do processo.
Papéis	Unidade de segurança da informação.
Entradas	Vulnerabilidades conhecidas e que afetem ativos de TIC da instituição.
Saídas	Registro de demanda para tratamento da vulnerabilidade.

Atividades	Registrar demanda	Registrar no sistema de gestão de demandas pendência para tratamento das vulnerabilidades conhecidas e/ou detectadas. Tal registro deve conter informações pertinentes às vulnerabilidades. Visando a eficiência do processo é possível e desejável que um registro possa abordar mais de uma vulnerabilidade, agrupando-as por sistema e/ou ambiente, sem prejuízo da rastreabilidade de tratamento. Se a vulnerabilidade for em imagem ou ativos de TIC, cuja configuração e versionamento seja nacional e de responsabilidade do CSJT ou de outro Tribunal, deve-se registrar a demanda no ambiente centralizado.
	Encaminhar demanda	Encaminhar a demanda à área de TIC responsável pelo ativo que possui a respectiva vulnerabilidade.
	Notificar CGSI	Notificar o Comitê Gestor de Segurança da Informação, quando a vulnerabilidade for classificada como de alta criticidade.

9.4 Avaliar demanda

Avaliar demanda	
Descrição	Avaliar demanda de tratamento de cada vulnerabilidade.
Papéis	Unidades de TIC
Entradas	Registro de demanda para tratamento da vulnerabilidade.
Saídas	Registro de demanda para tratamento da vulnerabilidade avaliado e escalado.

Atividades	Avaliar a vulnerabilidade	Avaliar a viabilidade do tratamento da vulnerabilidade, preferencialmente realizando testes em ambiente controlado, considerando os impactos que o tratamento pode acarretar e os recursos necessários. Também serão definidos os procedimentos de aplicação da correção e o de rollback. Se a vulnerabilidade for em imagem ou ativos de TIC, cuja configuração e versionamento seja nacional e de responsabilidade do CSJT ou de outro Tribunal, deve-se registrar a avaliação no ambiente centralizado.
	Atualizar chamado	Atualizar o chamado com as informações pertinentes, inclusive quanto à criticidade.
	Escalar tratamento	Quando viável escalar (programar) o tratamento da demanda, segundo a criticidade estabelecida.

9.5 Tratar vulnerabilidade

Tratar vulnerabilidade		
Descrição	Quando viável, realizar o tratamento da vulnerabilidade.	
Papéis	Unidades de TIC.	
Entradas	Registro de demanda de vulnerabilidade escalado.	
Saídas	Chamado de tratamento de vulnerabilidade atualizado.	
Atividades	Tratar	Quando viável, realizar as medidas necessárias para a correção da vulnerabilidade.

	Atualizar demanda	Atualizar a demanda com as informações pertinentes.

9.6 Fechar Demanda

Fechar Demanda		
Descrição	Atualizar a Base de Conhecimento e o Inventário de Ativos, quando for o caso.	
Papéis	Unidades de TIC.	
Entradas	Chamado de tratamento de vulnerabilidade com as informações pertinentes ao tratamento ou não da vulnerabilidade.	
Saídas	Atualização da Base de Conhecimento e do Inventário de Ativos, quando for o caso.	
Atividades	Atualizar Base de Conhecimento	Quando a vulnerabilidade for tratada, registrar na Base de Conhecimento o procedimento e as informações pertinentes.
	Atualizar Inventário	Quando necessário, atualizar as informações no Inventário de Ativos para os ativos de TIC afetados no tratamento da vulnerabilidade.
	Fechar demanda	Encerrar a demanda, informando se a vulnerabilidade foi tratada ou não.

9.7 Elaborar relatório

Elaborar relatório	
Descrição	Elaborar relatório anual de tratamento de vulnerabilidades e informar o Comitê Gestor de Segurança da Informação.
Papéis	Unidades de segurança da informação.

Entradas	Registro das demandas de tratamento de vulnerabilidades.	
Saídas	Relatório Anual de Tratamento de Vulnerabilidades.	
Atividades	Consultar demandas	Consultar os registros das de tratamento de vulnerabilidades do ano de referência.
	Calcular indicadores	Calcular os indicadores do processo.
	Editar relatório	Elaborar relatório com as informações obtidas.
	Encaminhar relatório ao CGSI	Encaminhar e apresentar o relatório ao Comitê Gestor de Segurança da Informação.

10. Indicadores de desempenho

Indicador 1	
Objetivo	Avaliar a eficácia do Processo de Gestão de Vulnerabilidades de TIC.
Indicador	Percentual de vulnerabilidades corrigidas em relação ao total de vulnerabilidades conhecidas que afetem os ativos de TIC da instituição.
Responsável	Unidade de segurança da informação.
Periodicidade	Anual.

Indicador 2

Objetivo	Avaliar a eficiência do Processo de Gestão de Vulnerabilidades de TIC.
Indicador	Média de tempo para atendimento dos chamados de tratamento de vulnerabilidade.
Responsável	Unidade de segurança da informação.
Periodicidade	Anual.

11. Anexos

11.1 Anexo I – Tabela de Classificação de Vulnerabilidades

Nível de criticidade	Descrição
Alto	O impacto da exploração pode afetar as atividades principais da instituição e os prejuízos decorrentes serão altos. Seu tratamento deve ser priorizado pelos gestores.
Médio	O impacto da exploração pode afetar uma parte das atividades da instituição e os prejuízos decorrentes serão razoáveis. Seu tratamento deve ser planejado pelos gestores.
Baixo	O impacto da exploração da vulnerabilidade pode afetar uma parte pequena e localizada das atividades da instituição e os prejuízos decorrentes serão baixos. Seu tratamento pode ser postergado a critério dos gestores.