Poder Judiciário
Tribunal Regional do Trabalho da 8ª Região
Secretaria de Tecnologia da Informação

Manual do Processo de Análise de Vulnerabilidades de Segurança da Informação

MAIO/2024

Poder Judiciário
Tribunal Regional do Trabalho da 8ª Região
Secretaria de Tecnologia da Informação

Histórico de Versões

Data	Descrição da Alteração	Responsável	Versão
06/05/2024	Criação do Documento.	Müller Miranda	1.0

Sumário

1. Objetivo do Processo

O processo "Análise de Vulnerabilidades de Segurança da Informação" do Tribunal Regional do Trabalho da 8ª Região tem por objetivo geral garantir que as vulnerabilidades presentes nos ativos tecnológicos sejam identificadas, analisadas, avaliadas, comunicadas, remediadas e/ou aceitas. Assim, permitir alcançar e manter o nível de exposição dos ativos dentro da faixa de valores aceitáveis ou adequados. Além disso, busca conscientizar e responsabilizar os proprietários dos ativos de TI.

2. Aplicação

As atividades e os resultados estabelecidos neste processo aplicam-se a todas as unidades do Tribunal, incluindo gestores, prestadores de serviços e contratados que tenham acesso e/ou utilizem ativos informacionais.

A Divisão de Segurança da Informação é responsável por elaborar, manter e fazer cumprir o processo no TRT da 8ª Região.

3. CVSS

A Common Vulnerability Scoring System (CVSS), ou Sistema de Pontuação Comum de Vulnerabilidades, é uma estrutura padrão para avaliar e classificar a gravidade das vulnerabilidades de segurança em sistemas de tecnologia da informação. Desenvolvido para fornecer uma medida uniforme e consistente do risco de segurança associado a uma vulnerabilidade, o CVSS atribui uma pontuação numérica a cada vulnerabilidade, facilitando a priorização de correções e a tomada de decisões em termos de segurança.

O CVSS avalia as vulnerabilidades com base em várias métricas, incluindo a facilidade de exploração, o impacto potencial e a complexidade da correção. A pontuação resultante fornece uma representação quantitativa do risco que uma vulnerabilidade representa, permitindo que as organizações priorizem suas ações de segurança de acordo com a gravidade percebida da ameaça.

Dentro de um processo de gestão de vulnerabilidades, o principal objetivo é mitigar os riscos associados a tais

vulnerabilidades, reduzindo a exposição de potenciais ataques e proteger os ativos de TI de uma organização.

4. Priorização de Correções

O tratamento de vulnerabilidades deve ser priorizado com base em sua classificação de risco e criticidade, tempo esperado para correção, grau de risco, impacto em caso de exploração e no valor que o ativo ou host impactado tem para o negócio do Tribunal Regional do Trabalho da 8ª Região.

5. Papéis e Responsabilidades

5.1. Equipe de Segurança da Informação - ESI

- Responsável por coordenar a execução de todos os tipos de varreduras (Redes Geral, Hosts Windows e Linux, Container, Aplicativos Web e Cloud), em todo o parque de ativos do Tribunal Regional do Trabalho da 8ª Região.
- Compilar mensalmente os resultados provenientes das varreduras periódicas, executadas pelos responsáveis dos ativos, realizadas no mês de referência.
- Acompanhar através dos indicadores de reação a ameaças o progresso da resolução de vulnerabilidades por grupos de responsabilidade.
- Acompanhar a Equipe de Operação no progresso de resolução das vulnerabilidades, auxiliando na análise do impacto e consequência do procedimento de resolução das vulnerabilidades por unidades e ativos.
- Gerar relatórios gerais e específicos, conforme as necessidades das áreas interessadas na diminuição dos riscos para os ativos estratégicos.
- Gerenciar a criação dos usuários e suas respectivas funções na ferramenta de gestão de vulnerabilidades, atribuindo permissões e perfis conforme necessário para acompanhamento das vulnerabilidades.

5.2. Responsáveis dos Ativos

- Prover informações necessárias para atualização do inventário de ativos, para detecção e análise das vulnerabilidades.
- Realizar varreduras periódicas (diária, semanal, mensal, contínua e isolada), conforme a importância e/ou criticidade dos ativos.

- Acionar a Equipe de Operação para correção das vulnerabilidades identificadas em varreduras. Devem acompanhar todo o ciclo de vida das vulnerabilidades encontradas, eliminando-as conforme a ordem de correção por prioridade.
- Prestar suporte na remediação das vulnerabilidades.

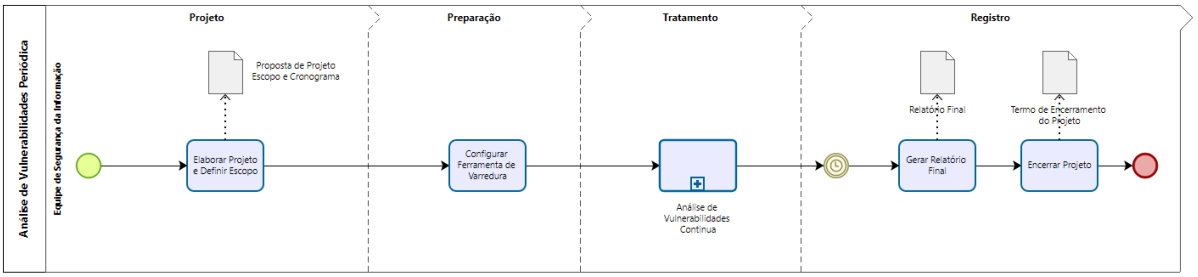
5.3. Equipe de Operação

- Executar os procedimentos de correções das vulnerabilidades para todos os ativos de rede (Servidores, Switches, roteadores, Hosts ESXs, Estações).
- Realizar análise dos procedimentos de correção das vulnerabilidades, identificando possíveis impactos e consequências, que tais procedimentos poderiam acarretar no ativo.
- Informar à ESI, sempre que novos serviços forem habilitados ou novos ativos forem inseridos na rede corporativa.
- Designar os grupos responsáveis pelos ativos cujas vulnerabilidades precisam ser acompanhadas durante todo seu ciclo de vida.

6. Processos

Este documento explora duas visões de processos. O primeiro refere-se a um escopo periódico, que se estende por um período considerável, geralmente um ano. O segundo é um processo contínuo, conduzido em ciclos mais breves, que se integra ao primeiro, de contexto mais amplo.

6.1. Análise de Vulnerabilidade Periódica



6.1.1. Descrição das Atividades

1 Projeto	
1.1	Elaborar Projeto e Definir Escopo
Objetivo	Elaborar um projeto com definição de escopo para uma análise e avaliação de vulnerabilidades para o ciclo de gestão.
Responsável	Equipe de Segurança da Informação
Procedimento	Escrever um documento definindo um período para execução do projeto e contendo escopo para análise e avaliação de vulnerabilidades.

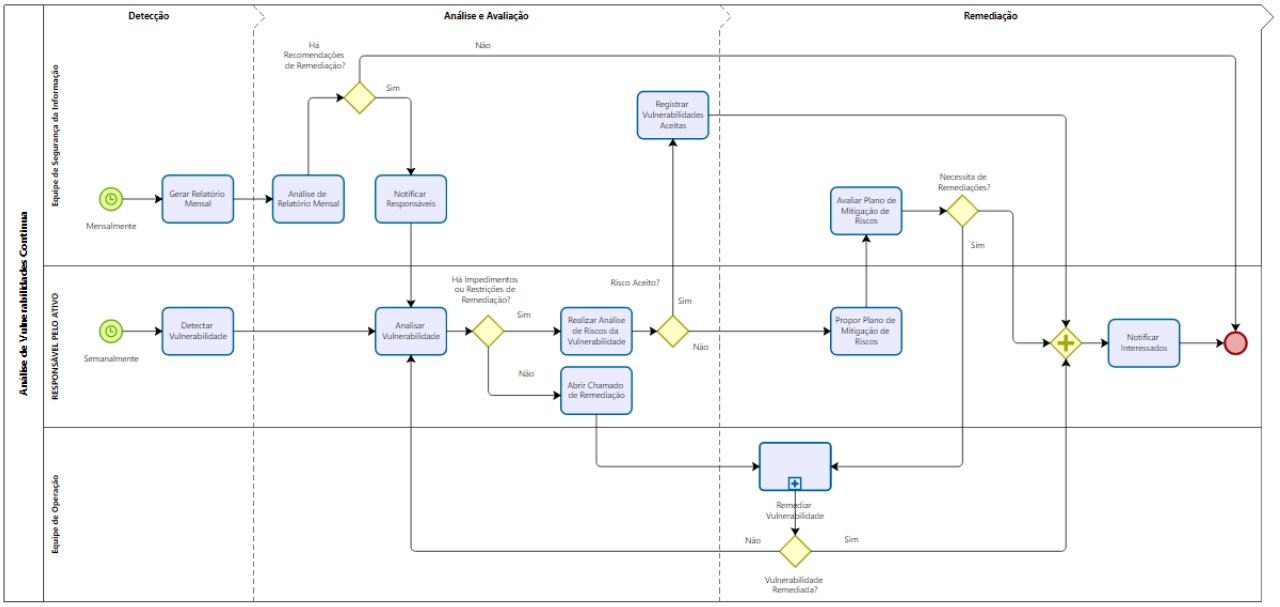
2 Preparação	
2.1	Configurar Ferramenta de Varredura
Objetivo	Configurar a ferramenta de varredura na solução de gerenciamento de vulnerabilidades para realizar a descoberta de ativos e detectar as vulnerabilidades presentes neles.
Responsável	Equipe de Segurança da Informação
Procedimento	Levantar as redes e os tipos de ativos que fazem parte do escopo; Configurar credenciais de serviço para os scans autenticados; Configurar sensores para fazer a descoberta de ativos nas redes; Definir janela de tempo para execução dos scans; Configurar scans agendados na ferramenta de varredura.

3	Tratamento
3.1	Análise de Vulnerabilidades Contínua

Objetivo	Subprocesso para identificar, avaliar e remediar potenciais vulnerabilidades de segurança em sistemas, redes, aplicativos e infraestrutura de forma contínua.
Responsável	Equipe de Segurança da Informação
Procedimento	Elaborar, manter e fazer cumprir o processo.

4 Registro	
4.1	Gerar Relatório Final
Objetivo	Apurar os resultados obtidos durante a execução do ciclo de gestão de vulnerabilidades.
Responsável	Equipe de Segurança da Informação
Procedimento	No final do ciclo de gestão de vulnerabilidades, deve ser gerado um relatório final contendo informações sobre os resultados obtidos com as ações e projetos para remediação das vulnerabilidades, inclusive com dados comparativos do cenário atual em relação ao início do ciclo e a ciclos anteriores.
4.2	Encerrar Projeto
Objetivo	Documentar todas as atividades relacionadas ao projeto.
Responsável	Equipe de Segurança da Informação
Procedimento	Comunicar formalmente o encerramento do projeto às partes interessadas, fornecendo um resumo das realizações, agradecimentos à equipe e próximos passos, se aplicável. Documentar as lições aprendidas ao longo do projeto, destacando sucessos, desafios e áreas de melhoria. Criar o Termo de Encerramento do Projeto.

6.2. Análise de Vulnerabilidade Contínua



6.2.1. Descrição das Atividades

1 Detecção	
1.1	Gerar Relatório Mensal
Objetivo	Compilar e apresentar as informações relevantes de um determinado período em um formato de relatório estruturado.
Responsável	Equipe de Segurança da Informação
Procedimento	A Equipe de Segurança da Informação deve estruturar o relatório de forma clara e organizada, dividindo-o em seções lógicas. Além disso, utilizar gráficos, tabelas ou outros elementos visuais para tornar os dados mais compreensíveis e atrativos.
1.2	Detectar Vulnerabilidade
Objetivo	Detectar as vulnerabilidades presentes nos ativos que fazem parte do escopo de responsabilidade da equipe responsável pelo ativo.

Responsável	Responsáveis dos Ativos
Procedimento	Planejar e executar scans periódicos (de preferência, semanalmente), para detectar as vulnerabilidades presentes nos ativos.

2 Análise e Avaliação	
2.1	Análise de Relatório Mensal
Objetivo	Servir como uma ferramenta para monitorar o desempenho organizacional e orientar o planejamento estratégico.
Responsável	Equipe de Segurança da Informação
Procedimento	A equipe de segurança da informação deve produzir e analisar relatório mensal e, se necessário, sugerir recomendações, tratamentos e investigações sobre as principais vulnerabilidades identificadas.
2.2	Notificar Responsáveis
Objetivo	O objetivo desta atividade é alertar sobre riscos inerentes às vulnerabilidades identificadas nos ativos e sugerir remediação.
Responsável	Equipe de Segurança da Informação
Procedimento	Envio de email e/ou abertura de chamado indicando os ativos e vulnerabilidades para serem tratadas.
2.3	Registrar Vulnerabilidades Aceitas
Objetivo	Manter o registro das vulnerabilidades aceitas
Responsável	Equipe de Segurança da Informação
Procedimento	Quando uma vulnerabilidade for aceitável pelos responsáveis do ativo, tanto pelo critério de severidade quanto pela avaliação de riscos, deve-se registar a aceitação na solução de gerenciamento de vulnerabilidades.

2.4	Analisar Vulnerabilidade
Objetivo	Analisar as vulnerabilidades identificadas e/ou comunicadas a fim de que sejam remediadas.
Responsável	Responsável pelo ativo
Procedimento	Os responsáveis pelos ativos devem verificar se há impedimentos ou restrições para remediação de cada vulnerabilidade e, havendo impedimentos, deve-se realizar a análise dos riscos envolvidos.
2.5	Realizar Análise de Riscos da Vulnerabilidade
Objetivo	Analisar os riscos das vulnerabilidades
Responsável	Responsáveis do Ativo
Procedimento	Quando houver impedimentos ou restrições para remediação em função de dificuldades técnicas, obrigações contratuais e normativas ou quaisquer exceções, deve-se realizar a análise dos riscos envolvidos a fim de avaliar se os riscos podem ser aceitos ou não. Vulnerabilidades aceitas devem ser revisadas periodicamente.
2.6	Abrir Chamado de Remediação
Objetivo	O objetivo desta atividade é formalizar e iniciar o processo de remediação de uma vulnerabilidade.
Responsável	Responsáveis do Ativo
Procedimento	Registrar chamado de remediação no Assyst indicando os ativos e vulnerabilidades a serem tratadas, indicando o procedimento a ser realizado (atualização, desinstalação, configuração, etc.)

3 Remediação	
3.1	Propor Plano de Mitigação de Riscos
Objetivo	Avaliar e propor estratégias para mitigar os riscos

	existentes de vulnerabilidades não aceitas.
Responsável	Responsáveis pelos ativos
Procedimento	Os responsáveis pelos ativos devem propor estratégias para mitigação das vulnerabilidades não aceitas.
3.2	Avaliar Plano de Mitigação de Riscos
Objetivo	A avaliação tem por objetivo propor ajustes caso necessário.
Responsável	Equipe de Segurança da Informação
Procedimento	A ESI deve avaliar o plano de mitigação de riscos de vulnerabilidades não aceitas, podendo propor ajustes caso julgar necessários.
3.3	Remediar Vulnerabilidade
Objetivo	Remediar vulnerabilidade seguindo o fluxo específico a fim de gerar o menor impacto possível nos serviços de TIC.
Responsável	Equipe de Operação
Procedimento	Considerando que as ações para remediação das vulnerabilidades podem ocasionar algum tipo de mudança nos serviços ou ativos de TIC, a fim de gerar o menor impacto possível aos usuários, o responsável pelo ativo deve acompanhar as ações de remediação.
3.4	Notificar Interessados
Objetivo	Informar as partes interessadas sobre os resultados relevantes das vulnerabilidades remediadas.
Responsável	Responsáveis pelos ativos
Procedimento	Notificar aos interessados o resultado da remediação das vulnerabilidades, seja por email ou descrição no chamado aberto no Assyst.