SUMÁRIO

1. INTRODUÇÃO

Um processo de gestão e análise de vulnerabilidades em TI é uma abordagem muito utilizada para identificar, avaliar, mitigar e monitorar as fraquezas ou falhas em processos, sistemas, softwares, infraestrutura, aplicativos, serviços e qualquer ativo de TI que possam ser exploradas por ameaças externas ou internas.

O processo de gestão e análise de vulnerabilidades na DTI do TCE-AL abrange a identificação de ativos e recursos, avaliação e priorização de vulnerabilidades, análise de riscos, mitigação das ameaças, aplicação de medidas de controles e correção de falhas, testes e validação das correções, monitoramento contínuo de novas ameaças e conscientização sobre a importância de manter a segurança física e lógica do ambiente de TI seguindo práticas definidas nas **Políticas de Gestão de Ativos, Riscos, Resposta a Incidentes, Controle de Acesso Lógico e Físico**. Este processo trata potenciais ameaças envolvendo diversos ativos de informação que sustentam os serviços da DTI, tais como: infraestrutura, sistemas, softwares, aplicações, aplicativos móveis, bancos de dados, sistemas de informação, dentre outros.

1.1. ESCOPO

O escopo do processo de gestão e análise de vulnerabilidades em TI abrange um conjunto de atividades que visam garantir a segurança e proteger os ativos de informação da DTI. Faz parte do escopo deste processo: identificação de ativos, inventário de software e hardware, descoberta e classificação de vulnerabilidades, avaliação de riscos, correção e mitigação, testes de controles de segurança, comunicação e divulgação de relatórios de monitoramento, acompanhamento contínuo, gestão de patches de correções, treinamento e conscientização.

1.2. OBJETIVO

O objetivo estratégico do processo de gestão e análise de vulnerabilidades em TI é fortalecer a estratégia de gestão de segurança da informação, reduzir o risco de exposição a ameaças e garantir a resiliência contra potenciais ataques cibernéticos, conforme diretrizes definidas nas

Políticas Corporativa de Segurança da Informação, Privacidade e Proteção de Dados Pessoais, Gestão de Riscos de TI. Neste sentido a DTI do TCE-AL tem a sua atuação direcionada pelos seguintes objetivos complementares:

a) identificar e catalogar todas as vulnerabilidades presentes nos sistemas, aplicativos, softwares e infraestrutura da DTI;

b) avaliar o risco associado a cada vulnerabilidade, considerando fatores como probabilidade de exploração e impacto potencial;

c) priorizar as vulnerabilidades com base em sua criticidade e no risco associado, permitindo a alocação eficiente de recursos para mitigar as ameaças mais críticas;

d) definir medidas para mitigar ou corrigir vulnerabilidades identificadas, seja por meio de aplicação de patches de correção seguindo a práticas descritas na **Política de Atualização de Softwares e Certificados Digitas**, configurações de segurança, atualizações de softwares ou outras ações.

1.3. ABRANGÊNCIA

O processo de gestão e análise de vulnerabilidades em TI é aplicável a todas as áreas da DTI do TCE-AL e abrange vários aspectos de segurança tais como: identificação de ativos, avaliação de riscos, varredura, deteção, priorização, mitigação e correção de vulnerabilidades, monitoramento contínuo, treinamento e conscientização, gestão e resposta a incidentes, análise de tendências e gestão de fornecedores.

1.4. BENEFÍCIOS ESPERADOS

A execução do processo de gestão e análise de vulnerabilidades em TI agrega valor e os seguintes benefícios:

a) permite identificar e corrigir vulnerabilidades antes que sejam exploradas por ameaças, reduzindo o potencial de ataques;

b) reduz a exposição a riscos, protegendo os sistemas e dados da DTI;

c) antecipa, mitiga vulnerabilidades e reduz o impacto de possíveis incidentes no ambiente operacional de TI;

d) melhoria contínua e confiabilidade dos sistemas e serviços oferecidos pela DTI;

e) ações proativas para gerenciar vulnerabilidades e demonstrar o compromisso com a segurança, preservando a reputação da DTI;

f) identifica e corrigi vulnerabilidades que podem levar a um ambiente de TI mais estável e eficiente, contribuindo para a produtividade geral da DTI;

g) estabelece uma cultura de segurança transparente, gerando confiança entre usuários e partes interessadas.

h) reduz os custos relacionados a recuperação de dados, interrupção de serviços e resposta a incidentes de segurança.

i) ajuda a manter a conformidade com a LGPD (Lei Geral de Proteção de Dados), evitando multas e penalidades, conforme diretrizes definidas nas **Políticas Corporativa de Segurança da Informação, Privacidade e Proteção de Dados Pessoais**.

2. ATRIBUIÇÕES E RESPONSABILIDADES

Da Diretoria DTI - compete à Diretoria de Tecnologia e Informática do TCE-AL as seguintes diretrizes:

a) pesquisar, implantar e manter, onde aplicável, soluções para gestão e análise de vulnerabilidades no âmbito da DTI;

b) pesquisar, gerenciar e coordenar a implantação e execução do processo de gestão e análise de vulnerabilidades em TI;

c) implantar, gerenciar e monitorar as ações de mitigação e /ou correção de vulnerabilidades em TI.

Do Núcleo de Segurança da Informação – compete ao Núcleo de Segurança da Informação do TCE-AL as seguintes diretrizes:

a) assessorar a Diretoria DTI na implantação do Processo de Gestão e Análise de Vulnerabilidades em TI;
b) incentivar estudos de novas tecnologias, bem como, seus eventuais impactos relacionados a vulnerabilidades em TI;
c) apoiar e acompanhar ações de correção e/ou mitigação das vulnerabilidades identificadas.

Dos Usuários/Colaboradores da TI – compete aos usuários/colaboradores seguir as seguintes diretrizes para não tornar os ativos de informação da DTI vulneráveis:

a) respeitar os princípios da finalidade e uso dos ativos de TI estabelecido na política e processos de segurança da informação;
b) utilizar os ativos de informação da DTI prioritariamente para a realização das atividades desempenhadas nos limites da ética, razoabilidade e legalidade;
c) não entregar dispositivos e equipamentos de TI em geral a pessoas sem autorização prévia.

Dos Fornecedores - responsáveis pela definição de boas práticas de configuração segura e correção de vulnerabilidades identificadas por eles ou pelas áreas que utilizam os ambientes, ferramentas e soluções de terceiros adquiridas pela DTI.

3. REFERÊNCIAS

Manual de Classificação e Tratamento de Informações Sigilosas;

Manual de Gerenciamento de Permissões de Acesso;

Norma ABNT ISO/IEC 20000:2018 para Gerenciamento de Serviços de TI;

Norma ABNT ISO/IEC 27001:2022 para Gestão da Segurança da Informação, Segurança Cibernética e Proteção à Privacidade;

Norma ABNT ISO/IEC 29134:2017 - Tecnologia da Informação - Técnicas de Segurança, Avaliação de Impacto de Privacidade;

Norma ABNT NBR ISO/IEC 27005:2023 - Gestão de Riscos de TI;

Norma ABNT NBR 14724: 2011 – Informação e Documentação – Apresentação Trabalhos Acadêmicos;

Plano Diretor de Tecnologia da Informação PDTI (2024-2026);

Política Corporativa de Segurança da Informação do TCE-AL;

Política de Atualização de Softwares e Certificados Digitas;

Política de Controle de Acesso Lógico e Físico;

Política de Desenvolvimento Seguro na DTI do TCE-AL;

Política de Gestão de Ativos na DTI do TCE-AL;

Política de Gestão de Riscos de TI;

Política de Governança de TI;

Política de Privacidade e Proteção de Dados Pessoais do TCE-AL;

Política de Respostas a Incidentes de TI;

Política de Tecnologia da Informação do TCE-AL;

Procedimento Operacional de Gestão de Mudanças.

4. CONCEITOS E DEFINIÇÕES

Para fins de compreensão dos termos utilizados neste processo serão aplicados os seguintes conceitos e definições:

Ameaça: conjunto de fatores externos com o potencial de causar dano ao ambiente de tecnologia da informação;

Análise de vulnerabilidades: verificação e exame técnico de vulnerabilidades para determinar onde estão localizadas e como foram exploradas;

Ataque: evento de exploração de vulnerabilidades, o qual, ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;

Ativo: tudo que tenha valor para a DTI, material ou não;

Ativos de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para a DTI;

Evento: qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação, ou seja, qualquer ocorrência dentro do escopo de TI que tenha relevância para a gestão dos serviços entregues ao cliente;

Evento de segurança: qualquer ocorrência identificada em um sistema, serviço, infraestrutura de TI que indique potencial falha do não atendimento aos requisitos das políticas e normas de segurança ou mesmo uma situação até então desconhecida e que possa se tornar relevante em termos de segurança;

Gestão de vulnerabilidades: processo cíclico e contínuo de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades;

Incidente: qualquer evento que cause ou possa causar uma interrupção não planejada (imprevista) de um serviço ou uma redução da qualidade do serviço prestado;

Resposta a incidentes: medidas tomadas para a preparação, detecção, resposta, contenção e recuperação de um incidente em TI, além de todas as atividades pós incidente e de conscientização;

Risco: mensurado em termos de impacto e probabilidade, trata-se da possibilidade de ocorrência de um evento com potencial de impactar o cumprimento dos objetivos;

Risco de segurança da informação: risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo na gestão das atividades na DTI;

Teste de invasão: metodologia para testar a eficácia e a resiliência de ativos através da identificação e exploração de fraquezas nos controles de segurança e da simulação das ações e objetivos de um atacante;

Teste de penetração (PENTEST): também conhecido como teste de intrusão é fundamental para a análise de vulnerabilidades e consiste em testar todos os sistemas em busca de, além das já verificadas na fase anterior, vulnerabilidades conhecidas e disponibilizadas por especialistas;

Vulnerabilidades: condição que, quando explorada, pode resultar em uma violação de segurança dos sistemas computacionais ou infraestrutura de TI, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha;

Usuários: qualquer indivíduo com direitos de acesso aprovado.

5. DIRETRIZES GERAIS

As diretrizes gerais deste processo contribuem para o atendimento dos pilares da gestão de segurança da informação na DTI a partir de práticas, métodos e ações de controle na proteção dos ativos de TI seguindo os requisitos definidos nas **Políticas Corporativa de Segurança da Informação, Privacidade e Proteção de Dados Pessoais, Gestão de Ativos na DTI,** conforme seguem:

a) A equipe de TI, servidores, prestadores de serviços, fornecedores e partes interessadas devem ser conscientizados sobre as melhores práticas de segurança, incluindo a identificação e mitigação de vulnerabilidades;

b) A DTI deve, onde aplicável e em intervalos planejados, monitorar continuamente os sistemas e serviços em busca de novas vulnerabilidades e garantir que as correções implantadas sejam eficazes;

c) Todos os colaboradores devem ser conscientizados sobre as normas e boas práticas de segurança para reduzir a probabilidade de exploração de vulnerabilidades por meio de ações não intencionais ou falhas de segurança.

6. PRINCÍPIOS

Este processo de gestão e análise de vulnerabilidades em TI considera os seguintes princípios:

a) garantia de confidencialidade, integridade, disponibilidade e autenticidade das informações sob custódia da DTI, com respeito as regras da transparência e atribuição de confidencialidade apenas nos casos expressamente previstos no **Manual de Classificação e Tratamento de Informações Sigilosas**;
b) alinhamento da **Política Corporativa de Segurança da Informação** com os demais planos e normativos institucionais do Tribunal;
c) conscientização, educação e comunicação como base fundamental para evolução da cultura em segurança da informação.

7. GESTÃO E ANÁLISE DE VULNERABILIDADES

O processo de gestão e análise de vulnerabilidades consiste em buscar, priorizar e corrigir vulnerabilidades em recursos, sistemas operacionais, infraestrutura, banco de dados, sistemas de informação, software, soluções e serviços de TI de forma a garantir que os ativos tenham condições seguras de uso, conforme diretrizes definidas na **Política de Gestão de Ativos na DTI**.

A gestão de vulnerabilidades deve permitir a implementação de mecanismos para obter informações oportunas sobre potenciais ameaças a infraestrutura, sistemas e ativos de informação, a análise da exposição da DTI a tais fragilidades e a adoção de salvaguardas apropriadas para lidar com os riscos associados.

A partir da execução das fases deste processo, abaixo descritas, a DTI pode diminuir suas superfícies de ataques, identificar e remover erros de configuração e problemas que possam ser explorados e gerenciar patches de segurança de sistemas e software, conforme diretrizes definidas nas **Políticas de Desenvolvimento Seguro** e **Atualização de Softwares e Certificados Digitais**.

7.1. IDENTIFICAÇÃO

Fase responsável por realizar o levantamento e a análise minuciosa dos sistemas, aplicativos, softwares, banco de dados, infraestrutura e processos para identificar possíveis falhas ou pontos fracos que possam ser explorados por ameaças. Ela envolve a execução das seguintes atividades:

a) manter um inventário atualizado (marca, modelo, versão) de todos os ativos de TI, incluindo, hardware, software, sistemas, bases de dados, para uma melhor compreensão do que precisa ser protegido, seguindo práticas definidas na **Política de Gestão de Ativos na DTI**;

b) realizar varredura de vulnerabilidades, sempre que possível e em intervalos planejados ou após alterações significativas no ambiente de TI, por equipe interna, terceiros, ferramentas automatizadas ou uma combinação de ambos;

c) preparar as ferramentas aplicadas nas varreduras de vulnerabilidades e verificar sua integridade de forma a evitar erros no mapeamento de brechas de segurança seguindo requisitos definidos na **Política de Resposta a Incidentes de TI**;

d) realizar testes de vulnerabilidades, sempre que possível, por meio de scanners, testes de penetração (PENTEST) e acompanhamento de alertas de segurança.

7.2. VERIFICAÇÃO / AVALIAÇÃO

Fase responsável por compreender o impacto e a criticidade das vulnerabilidades identificadas, priorizando as ações necessárias para mitigá-las. Ela envolve a execução das seguintes atividades:

a) coletar e analisar as informações disponíveis sobre vulnerabilidades, incluindo logs e outros registros gerados pelos recursos, sistemas e serviços de TI;

b) realizar varreduras automatizadas (autenticadas e não autenticadas) de vulnerabilidades nos ativos internos da DTI com frequência planejada;

c) avaliar a integridade dos resultados obtidos na detecção das vulnerabilidades;

d) identificar a existência de outros eventos e alertas relacionados com as vulnerabilidades em questão;

e) verificar que tipos de informações e processos podem ser afetados com as vulnerabilidades identificadas;

f) avaliar a relevância e o impacto das vulnerabilidades a fim de definir quais medidas devem ser tomadas para a remediação;

g) manter, dentro do possível, um banco de dados de vulnerabilidades coletadas de várias fontes como sites de segurança da informação, boletins de segurança ou publicações de fornecedores de softwares que precisam ser aplicadas aos ativos da DTI;

h) analisar regularmente as informações coletadas e mantidas no banco de dados de vulnerabilidades objetivando identificar tendências e padrões visando a tomada de medidas proativas para evitar fragilidades futuras;

i) classificar/categorizar a severidade das vulnerabilidades identificadas e atribuir a elas um nível de prioridade de acordo com a gravidade e o risco real.

7.3. REMEDIAÇÃO

Fase responsável por corrigir ou mitigar as vulnerabilidades identificadas e avaliadas com base na aplicação de correções, patches de segurança, atualizações de softwares ou implementação de contramedidas, conforme diretrizes definidas nas **Políticas de Resposta a Incidentes de TI, Atualização de Softwares e Certificados Digitais, Gestão de Riscos de TI**. Ela envolve a execução das seguintes atividades:

a) estabelecer e manter uma estrutura de remediação documentada e com revisões frequentes;

b) executar atualizações de aplicativos e no sistema operacional por meio do gerenciamento automatizado de patches de segurança com maior frequência;

c) tratar vulnerabilidades com base na priorização realizada a partir da classificação de risco e criticidade, tempo esperado para correção, grau de risco, impacto em caso de exploração e no valor que o ativo impactado tem para o negócio da DTI;

d) corrigir as vulnerabilidades detectadas por meio de processos e ferramentas em intervalos planejados;

e) implantar em produção, a partir do **Processo Operacional de Gestão de Mudanças**, somente as correções de vulnerabilidades que foram efetivamente testadas e aprovadas de forma que os controles apropriados em relação aos testes, avaliação de riscos e reparação sejam aplicados.

7.4. COMUNICAÇÃO

Fase responsável por garantir que todas as partes interessadas estejam cientes das vulnerabilidades identificadas, das medidas de remediação tomadas e das ações realizadas. Ela envolve a execução das seguintes atividades:

a) confirmar o restabelecimento da normalidade dos recursos computacionais após tratamento das vulnerabilidades;

b) registrar as ações realizadas durante o processo de remediação, incluindo as vulnerabilidades identificadas, as soluções aplicadas e os resultados dos testes;

d) registrar lições aprendidas e feedback com os usuários;

e) preparar relatórios detalhados sobre vulnerabilidades encontradas, análises de risco, ações tomadas e recomendações;

h) atualizar periodicamente políticas e procedimentos internos.

7.5. INTEGRAÇÃO COM A GESTÃO DE RISCOS

O processo de gestão e análise de vulnerabilidades deve estar totalmente integrado com as diretrizes definidas na **Política de Gestão de Riscos de TI**, alinhando as decisões sobre as tratativas de vulnerabilidades com a tolerância aos riscos que a DTI conduz.

8. DOS TIPOS GERAIS DE VULNERABILIDADES EM AMBIENTES DE TI

Na área de TI, as vulnerabilidades podem ocorrer por descuido humano, fraqueza em uma aplicação ou bug de implementação, permitindo que os dados sejam explorados por uma ou mais ameaças. Quanto mais cedo você descobrir as vulnerabilidades, mais tempo você terá para corrigi-las, ou ao menos para avisar o fabricante sobre a situação, reduzindo a grandeza que um atacante em potencial poderia ter. Neste sentido listamos abaixo alguns tipos de vulnerabilidades nos ambientes de TI que podem se manifestar de diversas formas e em diferentes níveis de gravidade mesmo cumprindo os requisitos definidos nas **Políticas Corporativa de Segurança da Informação**, **Privacidade e Proteção de Dados Pessoais**, **Desenvolvimento Seguro e Atualização de softwares e Certificados Digitais na DTI** :

8.1. SEGURANÇA DA INFORMAÇÃO

a) *Malware (a ameaça invisível):* representa uma das maiores ameaças de segurança em TI, sendo responsável por inúmeras violações. Neste sentido, é crucial estar ciente dos diferentes tipos de malware, como vírus, worms, trojans e ransomware, e adotar medidas de defesa adequadas;

b) *Ataques de Phishing (enganando através da manipulação)*: forma sofisticada de engenharia social onde os invasores tentam obter informações confidenciais por meio de e-mails, mensagens ou sites falsos. Neste sentido, aprender a reconhecer sinais (erros gramaticais, solicitações suspeitas de informações pessoais ou URLs estranhas) de um ataque de phishing é fundamental;

c) *Vulnerabilidades de Softwares (brechas na segurança)*: são pontos fracos que podem ser explorados por invasores, principalmente, quando os softwares de correção não estão atualizados. Desta forma é fundamental aplicar patches de segurança e utilizar ferramentas de detecção de vulnerabilidades para identificação das possíveis fragilidades;

d) *Engenharia Social (manipulação humana como estratégia)*: envolve a manipulação psicológica dos usuários para obter informações confidenciais. Assim sendo é fundamental estar atento a táticas como pretextos, solicitações urgentes e informações pessoais excessivas.

8.2. INFRAESTRUTURA DE TI

a) *Hardware Antigo*: erro muito comum que afeta a produtividade do time de TI, uma vez que, os equipamentos em geral tendem a ser mais lentos e suscetíveis a qualquer tipo de violação;

b) *Credenciais de Segurança:* erro básico que acarreta a perda de dados por conta da ausência de autenticação (senha forte) e criptografia de informações sensíveis;

c) *Software Ultrapassado*: outro problema muito comum que afeta a maioria dos dispositivos e equipamentos de TI por não ter suas versões mais recentes atualizadas;

d) *Firewall e Antivírus*: ausência de investimento e priorização na adoção de sistemas de firewall e antivírus seguros e eficientes aumenta a capacidade de pessoas mal-intencionadas de burlá-los, seja para roubar dados, seja para sequestrar equipamentos;

e) *Ineficiência de Backup:* ausência de backup em nuvem, preferencialmente gerenciado por uma empresa que tenha responsabilidade em garantir a segurança dos nossos serviços, afeta a confidencialidade, integridade, disponibilidade e autenticidade dos dados.

8.3. DESENVOLVIMENTO E SUSTENTAÇÃO DE SOLUÇÕES

a) *Quebra de Controle de Acesso:* ausência da abordagem de "privilégio mínimo", dando a cada usuário apenas as permissões necessárias para cumprir suas funções compromete todos os sistemas ativos no ambiente de TI;

b) *Falhas de Criptografia:* ausência de práticas de criptografia tais como algoritmos datados; chaves de criptografia fracas ou reutilizadas; descuido no gerenciamento e rotatividade de chaves afeta todos os dados trafegados nas aplicações de TI;

c) *Design Inseguro:* esta fragilidade é bem ampla e envolve ausência de biblioteca de componentes e padrões de design de segurança, modelagem de ameaças na hora de criar autenticações, controles de acesso, lógica de negócios e fluxos-chave, testes de unidade e de integração para garantir que todos os fluxos importantes são resistentes aos modelos de ameaça e linguagem e controle de segurança em histórias de usuários;

d) *Má Configuração de Segurança*: esta é a mais comum das fragilidades já listadas pois envolve desde configurações incompletas até falhas na configuração de cabeçalhos de páginas HTTP;

e) *Componentes Vulneráveis e Datados*: esta é uma fragilidade que precisa de um monitoramento constante e sistematizado, uma vez que, a grande maioria das vulnerabilidades

são escondidas em componentes de software que chamam pouco a atenção dos desenvolvedores;

f) *Falhas de Integridade de Dados e Software*: este tipo de fragilidade se refere a códigos e infraestrutura que não protegem contra violações de integridade a exemplo de programas que usem plugins, bibliotecas ou módulos de fontes não confiáveis;

g) *Insuficiência de Logs e Monitoramento*: esta fragilidade é alimentada principalmente pela ausência de logs com capacidade de detecção, preferencialmente em tempo real, de atividades suspeitas ou tentativas de acesso não autorizadas;

h) *Forja de Sever-Side Request (ataque e defesa*): Esta fragilidade permite que o usuário mal-intencionado force uma aplicação a enviar requisições de HTTP para qualquer domínio mesmo com soluções protegidas por firewall, VPN ou outros meios de controle de acesso.

i) Exploração de Vulnerabilidade da Versão de Linguagem de Programação: A utilização de versões desatualizadas de linguagens de programação pode introduzir várias fragilidades nos sistemas. Isso inclui vulnerabilidades de segurança conhecidas que não são corrigidas, falta de suporte oficial, incompatibilidades com novas bibliotecas e ferramentas, e perda de melhorias de performance que são introduzidas em versões mais recentes.

8.4. BANCO DE DADOS

a) Injeção de Código em Base de Dados: vulnerabilidade muito encontrada em banco de dados ou SQL onde o invasor encontra um parâmetro que passa pelo banco de dados e usa esse parâmetro para transportar um comando SQL malicioso como um conteúdo. O banco de dados armazena e o confunde como um código, enganando o software para enviar, alterar ou excluir o banco de dados.

b) Da mesma forma BD deve inserir ponto referente as vulnerabilidades versão do BD desatualizada

c) Controle de Acesso e Privilégios Exagerados: Aplicações ou usuários com permissões além das necessárias podem comprometer a segurança dos bancos de dados, conforme diretrizes definidas no **Manual de Gerenciamento de Permissões de Acesso**.

d) Injeção de código via Funções e Procedures armazenadas: a manipulação de procedures e funções armazenadas para executar comandos não autorizados.

9. TÉCNICAS PARA ANÁLISES DE VULNERABILIDADES

É recomendável a utilização de algumas técnicas para efetuar a identificação e análise das vulnerabilidades de TI. Geralmente são utilizadas em conjunto para investigar com maior profundidade um determinado evento de segurança e aplicáveis em todas as fases do processo de gestão de vulnerabilidades, conforme seguem:

a) Escaneamento de Portas – técnica utilizada para identificar portas abertas e serviços disponíveis em uma estrutura de processamento e transmissão de dados (host de rede) buscando fragilidades. Possibilita a equipe de infraestrutura e administradores da rede examinar a segurança dos sistemas, servidor ou ambiente TI enquanto atacantes a usam para identificar portas abertas com foco na exploração e / ou execução de serviços mal-intencionados.

b) Varredura de Vulnerabilidades – aplicativo de software que avalia vulnerabilidades em sistemas de informação (incluindo computadores, sistemas de rede, sistemas operacionais e aplicativos de software, versões de software, serviços e banco de dados) que possam ter sido originadas por um fornecedor, por atividades de administração do sistema ou ainda por atividades gerais de usuários no dia a dia. Essa ferramenta é alimentada por informações coletadas em base de dados de colaboração na internet e informações divulgadas por fabricantes de hardwares e softwares permitindo que os sistemas sejam sempre verificados pelas vulnerabilidades mais recentes divulgadas na comunidade.

c) Teste de Penetração - teste de penetração (PENTEST), envolve a simulação de ataques reais para avaliar o risco associado a possíveis violações de segurança. Nele os testadores não só descobrem vulnerabilidades que podem ser usadas por invasores, mas também exploram essas vulnerabilidades, sempre que possível, para avaliar o que os invasores podem obter após uma exploração bem-sucedida. Quando um teste de penetração é conduzido, consequentemente, se realiza uma varredura de vulnerabilidades. Isso ocorre porque a fase inicial requer que uma avaliação completa de vulnerabilidade seja conduzida para que os analistas responsáveis possam aprender os endereços IP, tipos de dispositivos, sistemas operacionais e quaisquer vulnerabilidades apresentadas pelos sistemas.

10. FERRAMENTAS PARA GESTÃO DE VULNERABILIDADES

Para auxiliar o processo de gestão de vulnerabilidades de TI, a automatização e adoção de sistemas e ferramentas de apoio é fundamental, conforme seguem:

a) Ferramentas de apoio na gestão de inventário - inventário de ativos de TI pode ser controlado manualmente quando os dados são informados pelo analista responsável, ou de forma automática quando são coletados através de agentes ou SNMP (Protocolo Simples de Gerência de Rede). Existem algumas técnicas e ferramentas que podem ajudar a manter este controle atualizado:

- FPING: semelhante ao comando PING (tempo que um sinal leva se deslocando do computador para um servidor e retornar) porém com um desempenho muito melhor para controle de endereçamento IP (protocolo de internet) em uso na rede;
- Zabbix Discovery Rules: ferramenta que faz a descoberta automática da rede, descobre IPs e mapeia serviços ativos sempre mantendo um histórico de eventos;

- Zabbix Host Inventory: ferramenta que descobre dispositivos baseados em agentes instalados nas máquinas controlando o tipo e função do ativo, nome, informações sobre sistema operacional, aplicativos e detalhes de hardware;
- Sistema Passivo de Detecção de Ativos em Tempo Real: escuta passivamente o tráfego de rede e reúne informações sobre equipamentos e serviços que estão ativos.
- OWASP ZAP (Zed Attack Proxy): Uma ferramenta de teste de penetração para aplicações web que ajuda a encontrar vulnerabilidades de segurança.

b) Ferramentas para análise de vulnerabilidades - análise de vulnerabilidades são basicamente efetuadas por softwares que integram uma ou mais ferramentas de segurança, conforme seguem:

- NMAP (mapeador de rede): utilitário de código aberto e licença gratuita para exploração de rede ou auditoria de segurança;
- NESSUS: scanner de vulnerabilidades de rede completo e inclui verificações de alta velocidade das fragilidades mais atualizadas, ampla variedade de opções de verificação, interface fácil de usar e relatórios eficazes;
- NIKTO: utilizado basicamente para varredura e testes de servidores web validando, no menor tempo possível, itens de configuração instalados.

11. PRIORIZAÇÃO E CORREÇÃO DE VULNERABILIDADES

O tratamento e correção 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 impactado tem para o negócio da DTI, em conformidade comas regras e etapas definidas na **Política de Gestão de Riscos de TI**.

Neste caso é essencial que se tenha uma prévia dos ativos prioritários da DTI antes de iniciar a análise e correção das vulnerabilidades. Tal priorização pode ser realizada por segmentos de rede, serviço, superfície de ataque ou a exposição da rede, levando-se em conta os benefícios que o devido tratamento da vulnerabilidade pode trazer ao ambiente de TI.

12. BANCO DE DADOS DE VULNERABILIDADES

Recomenda-se a implantação e manutenção de um banco de dados de vulnerabilidades coletadas de várias fontes, como sites de segurança da informação, boletins de segurança ou publicações de fornecedores de software, que precisam ser aplicadas aos sistemas e ativos da DTI.

O banco de dados poderá incluir informações de vulnerabilidades e plano de correção delas. Ele precisa ser atualizado regularmente com as informações mais recentes de vulnerabilidades tão logo sejam descobertas.

É recomendável que o banco de dados de vulnerabilidades seja integrado com outras ferramentas de segurança, como scanners de vulnerabilidades e sistemas de gerenciamento de patches possibilitando uma identificação e correção de forma mais rápida e eficiente.

As informações coletadas no banco de dados de vulnerabilidades devem ser analisadas regularmente para identificar tendências e padrões visando a tomada de medidas proativas para evitar futuras vulnerabilidades.

13. PRÁTICAS RECOMENDADAS PARA A GESTÃO DE VULNERABILIDADES

As práticas recomendadas para o processo de gestão e análise de vulnerabilidades em TI incluem:

a) normativos e procedimentos internos devem ser atualizados contendo diretrizes, competências e responsabilidades para identificação e controle de vulnerabilidades, a fim de prevenir ataques;

b) informações sobre vulnerabilidades técnicas dos sistemas e serviços em uso devem ser obtidas e a exposição da DTI a tais vulnerabilidades deve ser avaliada, tomando medidas adequadas;

c) um inventário atualizado de ativos na DTI seguindo as práticas da **Política de Gestão de Ativos** deve ser mantido e atualizado regularmente de forma a identificar vulnerabilidades presentes em sistemas operacionais, softwares, aplicativos, sistemas de informação e serviços de TI, utilizando ferramentas de escaneamento e testes de segurança;

d) vulnerabilidades identificadas devem ser classificadas e priorizadas com base no seu impacto potencial e na probabilidade de exploração, focando nas mais críticas e urgentes;

e) sistemas e softwares devem ser mantidos atualizados com as últimas correções de segurança, aplicando patches regularmente para fechar brechas conhecidas;

f) diretrizes da **Política de Controle de Acesso Lógico e Físico** e **Manual de Gerenciamento de Permissões de Acesso** devem ser seguidas controlando quem tem acesso a sistemas e dados sensíveis, reduzindo as chances de exploração por meio de acesso não autorizado;

g) ferramentas de monitoramento devem ser implementadas para fornecer alertas em tempo real sobre atividades suspeitas ou vulnerabilidades emergentes;

h) testes de invasão devem ser realizados regularmente e simulações de ataques devem ser feitas para avaliar a resistência dos sistemas e identificar possíveis brechas não detectadas;

i) diretrizes e regras definidas na **Política de Resposta à Incidentes de TI** devem ser serem seguidas em caso de violações de segurança, garantindo uma resposta rápida e eficaz;

j) usuários devem ser conscientizados sobre as boas práticas de segurança, pois muitas vulnerabilidades surgem de ações humanas inadvertidas;

k) uma comunicação clara e eficiente entre as equipes da DTI e outras partes interessadas devem ser mantidas para garantir ações coordenadas na gestão e análise de vulnerabilidades.

14. IMPLEMENTAÇÃO E MONITORAMENTO CONTÍNUO DAS VULNERABILIDADES

Uma das formas mais eficazes de garantir o monitoramento contínuo de vulnerabilidades de TI é utilizar as técnicas e ferramentas descritas nos itens **9 - TÉCNICAS PARA ANÁLISE DE VULNERABILIDADES e 10 - FERRAMENTAS PARA GESTÃO DE VULNERABILIDADES** acima citadas.

A implementação do referido monitoramento é fundamental para garantir a segurança dos sistemas e dados geridos pela DTI. Ao utilizar as referidas técnicas e ferramentas, automatizando a análise de logs, aplicando soluções de detecção de intrusões e realizando testes de penetração apropriadamente, haverá um fortalecimento e proteção do ambiente digital, bem como, mitigação dos riscos potenciais em tempo real.

Vale salientar que o monitoramento de vulnerabilidades de TI precisa ser contínuo e sistemático, bem como, exige atualizações regulares das técnicas e ferramentas utilizadas. Neste sentido, manter o processo de atualização sobre as últimas ameaças e tendências de segurança contribuirá para a eficácia contínua do monitoramento.

15. CONSCIENTIZAÇÃO E TREINAMENTO SOBRE VULNERABILIDADES

Recomenda-se a realização de práticas de conscientização de todos os servidores, colaboradores, prestadores de serviços, fornecedores, assim como treinamentos relativos às melhores práticas para uso de softwares e hardwares de propriedade da DTI, visando a proteção contra

vulnerabilidades. Esta medida irá contribuir para criação, desenvolvimento e manutenção de uma cultura de segurança em TI e comunicações internas, conforme diretrizes expressas na **Política Corporativa de Segurança da Informação**.

16. PENALIDADES

O não cumprimento das regras presentes neste processo de gestão e análise de vulnerabilidades de TI sujeita o colaborador às penalidades e sanções administrativas previstas nos normativos internos da DTI.

Casos omissos não tratados neste processo serão submetidos, analisados, tratados e decididos pela Diretoria DTI com apoio do Núcleo de Segurança da Informação.

17. IMPLEMENTAÇÃO E ATUALIZAÇÃO

Espera-se que o processo de gestão e análise de vulnerabilidades de TI seja revisado continuamente e, em intervalos planejados, seguindo as regras dos normativos internos da DTI, não se restringindo apenas a estes. Caso uma parte interessada identifique uma melhoria ela deve ser desenvolvida e implantada dentro do possível e onde for aplicável.

A DTI deve assegurar que as revisões deste processo sejam amplamente divulgadas com objetivo de promover a sua observância e cumprimento. Ademais, recursos humanos e tecnológicos devem ser disponibilizados para garantir a execução das regras nele contidos.

18. CONTROLE DE DOCUMENTOS E REGISTRO

Código	Responsável pela guarda	Permissão de acesso	Meio de arquivo	Indexação	Local de arquivo	Tempo de Arquivo	Forma de Disposição
PR-DTI-001	DTI	Restrito ao setor	Eletrônico	Alfabética	Base de Conhecimento	Permanente	Não aplicável

19. ANEXOS

Não se aplica.

20. HISTÓRICO DAS REVISÕES

Revisão	Descrição das alterações	Data
00	Emissão Inicial	23/07/2024
01	Formatação de texto	26/08/2024
02	Alteração de texto conforme sinalizações pontuadas pela Governança Coordenação e Líderes de Serviços.	30/10/2024

Elaborado por: **Equipe de Processos e Projetos**	Analisado e Aprovado por: **Diretoria DTI**
Data da Elaboração: 23/07/2024	Data da Aprovação: 21/11/2024