ANEXO XI
NORMA DE GESTÃO DE VULNERABILIDADES TÉCNICAS

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo

Versionamento:

Versão:	2.0
Data:	22/04/2024
Criada por:	Grupo de Trabalho Técnico (GTT) do CGSI
Aprovada por:	Comitê de Governança de Segurança da Informação (CGSI)
Aprovada em:	22/04/2024

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações
12/06/2023	1.0		
22/04/2024	2.0	GTT do CGSI	Conforme arquivo de registro de alterações (changelog).

1. INTRODUÇÃO

A Norma de Gestão de Vulnerabilidades Técnicas complementa a Política de Segurança da Informação, definindo diretrizes para execução de processos de monitoramento e tratamento de vulnerabilidades técnicas em todos os ativos de TIC do Poder Judiciário do Estado do Maranhão (PJMA).

Para fins desta norma aplica-se a lista de termos do glossário com suas respectivas definições, conforme descrito no ANEXO I - Glossário da PSI.

Esta norma obedece ao escopo definido na Política de Segurança da Informação.

2. OBJETIVO

Assegurar a integridade dos sistemas operacionais e mitigar a exploração de vulnerabilidades técnicas conhecidas.

3. DIRETRIZES

Estabelecer um processo contínuo e proativo para tratar riscos, realizar monitoramento, corrigir falhas e adotar medidas de proteção contra ameaças cibernéticas e violação de dados. Dessa forma, reduz-se a exposição do PJMA a riscos existentes e mitiga-se um número maior de vulnerabilidades.

As ações de proteção deverão ser sempre acompanhadas por ações de detecção e tomada de decisão sobre os ativos de TIC vulneráveis.

3.1 Gerenciamento de Vulnerabilidades

O gerenciamento de vulnerabilidades deverá ser criado, implementado, mantido e aplicado no PJMA e contempla:

I - estabelecer mecanismos para obter informações sobre vulnerabilidades técnicas dos sistemas e ativos de TIC, avaliação da exposição do PJMA a tais vulnerabilidades e a implementação de controles apropriados para tratamento do risco associado;

II - gerenciar os diversos ativos de TIC que sustentam os serviços do PJMA;

III - estabelecer funções e responsabilidades das equipes para realizar todas as atividades de maneira oportuna e eficaz para o PJMA;

IV - realizar atualizações de softwares, notificadas pelo fabricante ou fornecedor homologado, utilizando recursos autorizados, tais como: sítio eletrônicos de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.

3.2 Inventário de Ativos

O inventário de ativos de TIC, conforme estabelecido no ANEXO V - Norma de Gestão de Ativos da PSI, deverá ser incluído no escopo do gerenciamento de vulnerabilidades e patches. Ele deverá ser atualizado periodicamente ou sempre que ocorrerem alterações significativas, garantindo que os recursos informacionais estejam cobertos pelo gerenciamento de vulnerabilidades do PJMA.

3.3 Detecção de Vulnerabilidades

As ferramentas precisarão de configurações e ajustes adequados de acordo com o escopo avaliado. Da mesma forma, os tipos de detecções e testes terão que ser avaliados e ajustados para estar em conformidade com o escopo definido.

A frequência dos testes de segurança leva em consideração os requisitos legais, regulamentares e contratuais, bem como os riscos associados aos ativos de TIC do Poder Judiciário do Estado do Maranhão.

Os testes de segurança utilizarão o feed de vulnerabilidade mais recente para garantir a detecção abrangente de vulnerabilidades. Esses testes deverão ser realizados pela Diretoria de Informática e Automação (DIA) ou por uma empresa especializada, em horários que não impactem o uso dos recursos e sistemas disponibilizados pelo PJMA.

Para cada teste, deverá ser verificada a integridade da ferramenta utilizada, sua capacidade de analisar adequadamente as vulnerabilidades dos ativos de TIC, bem como identificar e tratar exceções.

As ferramentas utilizadas serão ajustadas continuamente para evitar discrepâncias nos resultados gerados por ferramentas distintas.

O teste de invasão ou de penetração (pentest) deverá ser realizado, periodicamente ou conforme necessidade do PJMA, incluindo o escopo da avaliação, os métodos de uso e os requisitos operacionais, a fim de fornecer as

informações mais precisas e relevantes sobre as vulnerabilidades atuais, sem afetar as atividades do PJMA.

A integridade do resultado sobre as detecções de vulnerabilidades deverá ser avaliada antes de sua comunicação, de forma a evitar inconsistências, contradições ou resultados incompletos. A detecção manual de vulnerabilidades será considerada como complemento às detecções automáticas. E, poderão ainda ser realizados novos testes de segurança para certificação do saneamento das vulnerabilidades encontradas.

3.4 Elaboração e Manutenção dos Relatórios de Vulnerabilidades

A Diretoria de Informática e Automação (DIA) deverá elaborar relatórios após cada ciclo de detecção para entender e mensurar as vulnerabilidades existentes. É essencial adotar métricas padronizadas internacionalmente ou amplamente utilizadas para os relatórios de vulnerabilidades, determinando o valor percentual dos ativos de TIC vulneráveis por gravidade.

Novas vulnerabilidades serão monitoradas levando em consideração sua severidade, tipo de ambiente, tipo de sistema, autoridade de numeração e tipo de vulnerabilidade.

O relatório resultante será classificado de acordo com a criticidade das informações contidas e poderá ser encaminhado ao Comitê de Governança da Segurança da Informação para avaliação e definição das ações necessárias.

3.5 Banco de Dados de Vulnerabilidades

Deverá ser mantido um banco de dados de vulnerabilidades, atualizado regularmente com informações coletadas de várias fontes, para ser aplicado aos sistemas e ativos de TIC do Poder Judiciário do Estado do Maranhão. Este banco de dados poderá incluir detalhes sobre as vulnerabilidades, análises para priorização e planos de correção, proporcionando uma visão abrangente das medidas necessárias para mitigar os riscos de segurança.

3.6 Priorização e Correção de Vulnerabilidades

O tratamento de vulnerabilidades deverá ser priorizado com base em sua classificação de risco e criticidade, tempo esperado para correção, impacto em caso de exploração e no valor que o ativo de TIC tem para o Poder Judiciário do Estado do Maranhão.

As vulnerabilidades deverão ser tratadas de acordo com o seu nível de severidade e nos prazos estipulados no quadro abaixo:

Nível de severidade	Prazo de correção	Descrição do risco
Muito Crítico (6)	Até 02 dias	Situação inaceitável. Ações imediatas serão necessárias para eliminar o risco e reduzir os potenciais perigos e impactos.
Crítico (5)	Até 15 dias	Indivíduos mal-intencionados poderão facilmente assumir o controle dos ativos de TIC, colocando em risco toda a rede de dados do PJMA. As vulnerabilidades incluem acesso não autorizado a arquivos, execução remota de comandos e backdoors.
Alto (4)	Até 30 dias	Existe o risco de indivíduos mal-intencionados adquirirem controle dos ativos de TIC ou coletarem informações altamente confidenciais, como acesso de "leitura" a arquivos, backdoors ou lista de contas de usuários(as).
Médio (3)	Até 45 dias	Indivíduos mal-intencionados poderão obter acesso às configurações de segurança nos ativos de TIC, permitindo o acesso não autorizado a arquivos, navegação em diretórios e ataques de negação de serviço.
Baixo (2)	Até 60 dias	Há o risco de coleta de informações sobre os ativos de TIC, revelando vulnerabilidades conhecidas, como versões de software instaladas.
Muito baixo (1)	Até 90 dias	Existe a possibilidade de coletar informações sobre os ativos de TIC por meio de serviços ou portas de conexão de rede abertas, resultando na descoberta de outras vulnerabilidades.

Quadro 1: Nível de severidade e prazos de correção

Os testes que forem concluídos com falha deverão ser revisados até que sua execução seja concluída com êxito. Caso não seja possível, deverá ser avaliado se a vulnerabilidade será incluída na lista de exceções, conforme o processo de aceitação de risco.

Deverão ser estabelecidos mecanismos para obtenção regular de atualizações de software quando emitidas pelo fabricante ou fornecedor oficial, utilizando recursos autorizados, tais como sítios eletrônicos de fornecedores de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.

Os alertas de vulnerabilidades, os patches de correções, as aplicações de atualizações e as ameaças emergentes que correspondam aos recursos informacionais relacionados no inventário de sistema e ativos de TIC deverão ser monitorados.

3.7 Das Exceções de Vulnerabilidades

Para os ativos de TIC do Poder Judiciário do Estado do Maranhão não contemplados por esta norma em função de dificuldades técnicas ou obrigações contratuais e normativas ou quaisquer exceções a esta norma, deverão ser documentadas e aprovadas.

3.8 Das Correções de Vulnerabilidades

As correções bem-sucedidas de vulnerabilidades poderão ser testadas por meio de detecção de vulnerabilidades de rede e de host, verificação de logs de patches, testes de invasão/penetração (pentest) e verificação das definições de configuração.

3.9 Implementação e Verificação das Correções de Vulnerabilidades

Somente correções de vulnerabilidades que foram efetivamente testadas e aprovadas deverão ser implantadas em produção. Atividades de correção de vulnerabilidades geralmente incluem, mas não se limitam à instalação de patches de segurança, aplicações de atualizações, bem como a ajustes de configuração e/ou remoção de software.

Quando instalações de patches de segurança e ajustes de configuração forem recomendadas para mitigar as vulnerabilidades, elas deverão seguir procedimento interno, devidamente documentado.

4. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

4.1 Diretoria de Informática e Automação

Compete à Diretoria de Informática e Automação:

I - observar o inventário de ativos de TIC definidos no ANEXO V - Norma de Gestão de Ativos da PSI;

II - classificar e tratar continuamente as vulnerabilidades existentes nos ativos;

III - priorizar as ações de correção e mitigação, avaliando o nível de ameaça e criticidade das vulnerabilidades;

IV - acompanhar notificações, alertas e recomendações emitidas, como Common Vulnerabilities and Exposures (CVE) ou registros similares, para executar ações necessárias;

V - estabelecer o gerenciamento de patches, atualizações, configurações e correções de vulnerabilidades.

As diretrizes para correção ou mitigação, assim como os procedimentos para aplicação de medidas corretivas, deverão ser definidos em normativo interno.

5. INFRAÇÕES E PENALIDADES

Infrações e penalidades serão aplicadas conforme previsto na Política de Segurança da Informação.

6. REVISÕES

Esta norma será alterada mediante necessidade de atualização, com apreciação e aprovação do Comitê de Governança de Segurança da Informação (CGSI).

7. APROVAÇÃO

A norma foi aprovada pelo Comitê de Governança de Segurança da Informação (CGSI), revogando-se todas as disposições em contrário.