JUSTIÇA FEDERAL
CONSELHO DA JUSTIÇA FEDERAL

PORTARIA N. 148-CJF

Dispõe sobre a implantação de norma de gestão de vulnerabilidades cibernéticas no âmbito do Conselho da Justiça Federal.

O PRESIDENTE DO CONSELHO DA JUSTIÇA FEDERAL, no uso de suas atribuições legais e regimentais, e

CONSIDERANDO a Resolução CNJ n. 396/2021, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Resolução CNJ n. 370, de 28 de janeiro de 2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO a Resolução CJF n. 687, de 15 de dezembro de 2020, que dispõe sobre a implantação da Política de Segurança da Informação do Conselho e da Justiça Federal de 1º e 2° graus;

CONSIDERANDO a Portaria CNJ nº 162, de 10 de junho de 2021, que aprova Protocolos e Manuais criados pela Resolução CNJ n. 396/2021, bem como prevê a necessidade do gerenciamento contínuo de vulnerabilidades para a proteção de infraestruturas críticas de TIC e para a prevenção e mitigação de ameaças cibernéticas;

CONSIDERANDO que os ataques cibernéticos se têm tornado cada vez mais avançados e com alto potencial de prejuízo, cujo alcance e complexidade não têm precedentes; que os impactos financeiros, operacionais e de reputação podem ser imediatos e significativos; e que é fundamental aprimorar a capacidade de prevenir ataques e identificar vulnerabilidades as quais poderiam ser exploradas por atacantes;

CONSIDERANDO que as vulnerabilidades de segurança que afetam a confidencialidade, integridade e disponibilidade das soluções de Tecnologia da Informação – TI são amplas e variadas,

RESOLVE:

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Implantar a norma de gestão de vulnerabilidades cibernéticas, em consonância com a Política de Segurança da Informação do Conselho e da Justiça Federal de 1º e 2º graus.

Art. 2º Esta norma orienta os responsáveis por estabelecer políticas e diretrizes para a gestão e gerentes de TI, bem como as equipes atuantes na gestão, administração, identificação e correção de vulnerabilidades de segurança nas soluções e sistemas de TI.

DOS OBJETIVOS

Art. 3º O objetivo geral da gestão de vulnerabilidades é reduzir os riscos de ataques cibernéticos em razão da exploração de vulnerabilidades cibernéticas conhecidas e ser componente-chave no planejamento e na implementação apropriada de controles de segurança para o gerenciamento de riscos.

Art. 4º São objetivos específicos do gerenciamento de vulnerabilidades:

I – obtenção de informações confiáveis sobre vulnerabilidades descobertas em soluções de TI;

II – identificação das vulnerabilidades existentes no ambiente tecnológico do Conselho da Justiça Federal;

III – classificação e priorização das vulnerabilidades identificadas;

IV – adoção de controles para minimizar o impacto ou a probabilidade de exploração das vulnerabilidades mais relevantes;

V – promoção da capacidade de resiliência cibernética.

DA PREPARAÇÃO

Art. 5º O processo de gestão de vulnerabilidades cibernéticas possuirá escopo apropriado para as capacidades operacionais das equipes do CJF e priorização conforme a Cadeia de Valor do Conselho da Justiça Federal e os serviços críticos de TI.

Art. 6º Fazem parte do escopo do processo de gerenciamento de vulnerabilidade cibernéticas, segundo a ordem de criticidade:

I – vulnerabilidades expostas à internet;

II – vulnerabilidades de fácil exploração;

III – vulnerabilidades em ativos de infraestrutura crítica de TI;

IV – vulnerabilidades massivas.

Art. 7º O inventário completo e atualizado dos ativos de informação é pré-requisito para a gestão efetiva das vulnerabilidades técnicas e deve identificar, no mínimo, todos os ativos de hardware, software, serviços em nuvem, o grau de criticidade e o respectivo responsável pela sua gestão.

DA VERIFICAÇÃO DE VULNERABILIDADES

Art. 8º Serão realizadas varreduras periódicas em todo ambiente tecnológico, de forma automatizada, para identificar vulnerabilidades sob a perspectiva de um atacante externo ou de um atacante na rede interna.

Art. 9º As verificações externas e internas serão preferencialmente executadas utilizando autenticação para permitir análises mais completas.

DA AVALIAÇÃO E TRATAMENTO DAS VULNERABILIDADES

Art. 10. As vulnerabilidades identificadas na varredura automatizada serão registradas em repositório de dados centralizado e categorizadas de acordo com, no mínimo, os seguintes critérios:

I – utilização da métrica internacional *Common Vulnerability Scoring System* (CVSS), que fornece uma representação numérica de 0 a 10, relativa à gravidade da vulnerabilidade;

II – utilização da base pública *Common Vulnerabilities and Exposures* (CVE) de falhas de segurança para identificação das vulnerabilidades identificadas;

III – identificação quanto à existência de algum programa ou código projetado para explorar a vulnerabilidade identificada (*exploit*).

Art. 11. As vulnerabilidades serão classificadas conforme a criticidade estabelecida no art. 6º desta Portaria e priorizadas em matriz cujos critérios sejam de gravidade, urgência, tendência e esforço.

Art. 12. As vulnerabilidades identificadas, classificadas e priorizadas constarão de base das principais vulnerabilidades cibernéticas para fins de acompanhamento e comunicação à alta administração.

Art. 13. Na base das principais vulnerabilidades cibernéticas será designado o responsável, identificada a causa-raiz, estabelecido o prazo para remediação ou tratamento, bem como definida a ação referente a cada vulnerabilidade principal, o que poderá consistir em:

I – mudança da configuração no ambiente;

II – aplicação da solução de contorno;

III – implantação de solução ou serviço;

IV – aceitação do risco.

Art. 14. Em relação ao tratamento das vulnerabilidades serão observados:

I – o processo de tratamento e resposta a incidentes de segurança;

II – a realização de testes e homologação da correção da vulnerabilidade técnica antes da aplicação em ambiente de produção;

III – se as alterações de configuração no ambiente motivadas pelas correções das vulnerabilidades técnicas foram implantadas de acordo com o processo de gestão de mudanças.

DO MONITORAMENTO DE VULNERABILIDADES

Art. 15. As informações divulgadas sobre vulnerabilidades e a aplicabilidade das medidas de segurança recomendadas serão verificadas periodicamente.

Art. 16. São fontes de consulta preferenciais:

I – vulnerabilidades divulgadas pelos fabricantes das soluções de TI utilizadas no Órgão;

II – vulnerabilidades divulgadas por fabricantes e empresas especializadas em segurança da informação;

III – boletins de equipes governamentais de resposta a incidentes;

IV – fóruns e sites especializados.

Art. 17. Os controles relacionados a seguir serão aplicados para a análise crítica dos resultados da gestão de vulnerabilidades:

I – comparação regular dos tempos de tratamento das vulnerabilidades para verificar se foram corrigidas em tempo hábil;

II – acompanhamento regular do nível geral de risco do ambiente tecnológico;

III – comunicação à Comissão Local de Segurança da Informação – CLSI a respeito da evolução, dos riscos e dos achados dos testes e das varreduras;

IV – proposição de melhorias nos processos da gestão de vulnerabilidades para a CLSI.

DOS RESPONSÁVEIS

Art. 18. Para assegurar a rastreabilidade adequada das vulnerabilidades, as responsabilidades e competências serão segregadas, observados os seguintes parâmetros:

I – cabe às áreas responsáveis pela administração de soluções de TI monitorar as vulnerabilidades disponibilizadas pelos fabricantes das soluções e aplicar as respectivas atualizações de segurança (*patch management*);

II – a Subsecretaria de Segurança da Tecnologia da Informação é responsável pela varredura e classificação de vulnerabilidades cibernéticas, por monitorar fontes de consulta relacionadas a vulnerabilidades cibernéticas e medidas de tratamento, pelo acompanhamento do tratamento das vulnerabilidades e pela análise crítica e proposição de melhorias no processo de gestão de vulnerabilidades;

III – a Seção de Suporte a Serviços é encarregada em aplicar regularmente as atualizações de segurança dos sistemas operacionais e em, centralmente, atualizar os aplicativos instalados nas estações de trabalho;

IV – o Comitê Gestor de Tecnologia da Informação é incumbido em priorizar e definir os responsáveis pelas ações de tratamento das vulnerabilidades priorizadas.

DAS DISPOSIÇÕES FINAIS

Art. 19. Os relatórios e registros gerados pertinentes à gestão de vulnerabilidades cibernéticas serão tratados e armazenados de forma segura e com acesso reservado às unidades envolvidas.

Art. 20. Serão realizados, periodicamente, testes de invasão para fins de validação da gestão de vulnerabilidades e dos controles de segurança aplicados.

Art. 21. Os casos omissos serão resolvidos pela Comissão Local de Segurança da Informação.

Art. 22. Esta Portaria entra em vigor na data de sua publicação e a sua implementação se dará no prazo de três meses subsequentes a essa data.

Ministro **HUMBERTO MARTINS**
Presidente

Autenticado eletronicamente por **Ministro HUMBERTO EUSTÁQUIO SOARES MARTINS**, **Presidente**, em 22/03/2022, às 14:27, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.cjf.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0318298** e o código CRC **8DF5652B**.
