INSTRUÇÃO NORMATIVA Nº 308, DE 23 DE OUTUBRO DE 2024.

Institui o Processo de Gestão de Vulnerabilidades baseado em Riscos da Segurança da Informação do Supremo Tribunal Federal.

***O DIRETOR-GERAL DA SECRETARIA DO SUPREMO TRIBUNAL FEDERAL**, no uso da atribuição que confere o art. 41, X, b, do Regulamento da Secretaria de 2024, considerando o disposto na Resolução 773/2022, que dispõe sobre a Política de Segurança da Informação e o que consta do Processo Administrativo eletrônico 009268/2024,*

R E S O L V E:

Art. 1º O Processo de Gestão de Vulnerabilidades Baseado em Riscos de Segurança da Informação (PGV-SI) do Supremo Tribunal Federal (STF) fica instituído por esta instrução normativa.
Parágrafo único. Para os efeitos desta instrução normativa, aplica-se o glossário de termos de segurança da informação definido no Repositório Digital constante do portal do STF.

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 2º Esta norma tem por finalidade estabelecer fluxos de tratamento de vulnerabilidades, bem como permitir sua identificação, detecção e classificação, para possibilitar a sua eliminação, quando possível, ou sua mitigação por meio de controles.
Parágrafo único. Os fluxos de tratamento de vulnerabilidades estão alinhados ao processo de Gestão de Riscos de Segurança da Informação do Tribunal.

Art. 3º O objetivo do PGV-SI é estabelecer as responsabilidades e o processo para a gestão de Vulnerabilidades de Segurança da Informação do Tribunal.

CAPÍTULO II
DAS RESPONSABILIDADES PARA A GESTÃO DE VULNERABILIDADES DE SEGURANÇA DA INFORMAÇÃO

Art. 4º Os responsáveis pelos ativos de informação deverão:
I – acompanhar as mensagens e os boletins disponibilizados pelos fabricantes e fornecedores, de forma a tomar ciência de novas vulnerabilidades que possam afetar os ativos sob sua responsabilidade;
II – garantir a configuração mínima necessária para o funcionamento dos ativos de informação, desabilitando serviços, funcionalidades e portas que não sejam essenciais, conforme as práticas recomendadas de fortalecimento de segurança (hardening);
III – manter atualizados os componentes, os softwares de terceiros e os sistemas operacionais dos ativos de informação sob sua responsabilidade, ativando as configurações de atualização automática, quando possível.

Parágrafo único. Os responsáveis pelos ativos de informação devem informar a Coordenadoria de Segurança Cibernética da Secretaria de Tecnologia e Inovação (STI) nos casos em que não seja possível atualizar os sistemas e componentes.

Art. 5º Cabe à Coordenadoria de Segurança Cibernética da STI:
I – acompanhar boletins nacionais e internacionais de Centros de Resposta a Incidentes, com intuito de informar, aos responsáveis pelos ativos, as principais vulnerabilidades exploradas que possam afetar os ativos sob suas responsabilidades;
II – registrar vulnerabilidades, em sistemas informatizados, que possam afetar os ativos do STF;
III – auxiliar os responsáveis pelos ativos na eliminação de vulnerabilidades, ou na seleção de controles que possam diminuir a probabilidade ou o impacto de sua exploração, em casos em que não seja possível a sua eliminação;
IV – identificar novas vulnerabilidades no ambiente por meio de varreduras periódicas e automatizadas com ferramenta que utilize o protocolo compatível com protocolo de automação de conteúdo de segurança (SCAP).
§1º A varredura de novas vulnerabilidades pode ser realizada por empresa terceira especializada, contratada para esse fim, ou via contratação específica.
§2º As varreduras devem ser realiza
das utilizando conta serviço dedicada, não utilizada para outros fins.

CAPÍTULO III
DO PROCESSO DE GESTÃO DE VULNERABILIDADES DE SEGURANÇA DA INFORMAÇÃO

Art. 6º Toda nova vulnerabilidade identificada deve ser registrada em sistema informatizado, contendo:
I – código CVE (Common Vulnerabilities and Exposures) da vulnerabilidade, quando disponível;
II – criticidade da vulnerabilidade, quando disponível;
III – descrição de como a vulnerabilidade foi identificada;
IV – ativos de informação afetados pela vulnerabilidade.
Parágrafo Único. A Coordenadoria de Integridade Digital da Secretaria de Relações com a Sociedade (SRS) deve ter acesso ao sistema informatizado.

Art. 7º As vulnerabilidades serão classificadas de acordo com sua criticidade, utilizando-se o Common Vulnerability Scoring System (CVSS) da seguinte forma:
I – nível crítico, caso a nota CVSS seja de 9 a 10;
II – nível elevado, caso a nota CVSS seja de 7 a 8.9;
III – nível moderado, caso a nota CVSS seja de 4.0 a 6.9;
IV – nível baixo, caso a nota CVSS seja de 0.1 a 3.9;
Parágrafo único. Preferencialmente, deve ser utilizada a nota CVVSv4, seguida da nota CVVSv3 e CVVSv2, caso a primeira não esteja disponível.

Art. 8º As vulnerabilidades identificadas não tratadas devem ser reportadas para os níveis hierárquicos superiores, considerando aspectos sobre a sua exploração e a exposição dos ativos ao ambiente externo do STF.
§1º O relatório das vulnerabilidades reportadas deve conter as justificativas de não tratamento, quando for o caso.
§2º A qualquer tempo, os membros do Comitê de Segurança da Informação poderão consultar as vulnerabilidades existentes por meio de um painel de gestão em sistema informatizado.

Art. 9º O relatório de identificação, mitigação e tratamento de vulnerabilidades deverá ser enviado pela STI, a pedido da Coordenadoria de Integridade Digital/SRS.

Art. 10. As vulnerabilidades de nível crítico que afetem sistemas críticos que porventura não puderem ser corrigidas devem ser objeto de avaliação de riscos de forma a selecionar controles que possam atuar na mitigação da probabilidade e do impacto de sua exploração.

Art. 11. Esta instrução normativa entra em vigor na data de sua publicação.

Publicada no DJE/STF em 25/10/2024.