SUPERIOR TRIBUNAL DE JUSTIÇA

INSTRUÇÃO NORMATIVA STJ/GDG N. 27 DE 18 DE NOVEMBRO DE 2024.

Regulamenta a gestão de vulnerabilidades de Tecnologia da Informação e Comunicação no âmbito do Superior Tribunal de Justiça.

O DIRETOR-GERAL DA SECRETARIA DO SUPERIOR TRIBUNAL DE JUSTIÇA, usando da atribuição conferida no 19.3, inciso X., alínea "b", do Manual de Organização do STJ,

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

CONSIDERANDO a Portaria CNJ n. 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 a Resolução STJ/GP n. 12 de 27 de abril de 2023, que institui a Política de Segurança da Informação do Superior Tribunal de Justiça;

CONSIDERANDO a Instrução Normativa STJ/GDG n. 17 de 26 de outubro de 2021, que institui a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação - Etir do STJ;

CONSIDERANDO a Instrução Normativa STJ/GP n. 5 de 15 de fevereiro de 2023, que institui os Comitês de Governança de TIC, Gestor de TIC e Gestores de Sistemas administrativos e judiciários;

CONSIDERANDO a Instrução Normativa STJ/GDG n. 4 de 6 de fevereiro de 2020, que regulamenta a Política de Gestão de Riscos do STJ;

CONSIDERANDO o que consta do processo SEI STJ n. 011412/2024,

RESOLVE:

Seção I

Das Disposições Preliminares

Art. 1º A gestão de vulnerabilidades de Tecnologia da Informação e Comunicação – TIC, fica regulamentada por esta instrução normativa.

§ 1º A gestão de vulnerabilidades de TIC estabelece as regras relacionadas às atividades de identificação, avaliação, documentação, comunicação e remediação de vulnerabilidades.

§ 2º A gestão de vulnerabilidades cibernéticas se aplica aos ativos de TIC do STJ, bem como a todas/os as usuárias e os usuários internas/os e instituições integradas.

Seção II

Das Definições

Art. 2º Para os efeitos desta instrução normativa, considera-se:

I – segurança da informação: ações que objetivam assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações;

II – ativos de Tecnologia da Informação e Comunicação – TIC: bens, sistemas e serviços de tecnologia da informação e comunicação que integrem a infraestrutura tecnológica do Tribunal;

III – segurança cibernética: conjunto de processos, boas práticas e soluções tecnológicas que objetivem proteger os ativos de TIC;

IV – vulnerabilidade cibernética: condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores:

a) suscetibilidade ou falha do sistema;

b) acesso possível à falha;

c) capacidade de explorar essa falha;

V – vulnerabilidade de dia zero: falha na segurança de um software, que ainda não é conhecida por seus desenvolvedores, pelos fabricantes de soluções de segurança e pelo público em geral, sendo, também, considerada uma vulnerabilidade de dia zero a falha de segurança que já é conhecida pelo fornecedor do produto, mas para cuja correção ainda não existe um pacote de segurança;

VI – *exploit*: técnicas, programas ou parte de programas maliciosos projetados para explorar uma vulnerabilidade existente em um programa de computador;

VII – incidente de segurança da informação: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança da informação de dados, sistemas de informação, *softwares*, dispositivos móveis e a dispositivo da infraestrutura de tecnologia da informação de propriedade do STJ, hospedado no datacenter ou na nuvem do Tribunal, ou sob sua guarda;

VIII – incidente crítico de segurança da informação: qualquer incidente de segurança da informação em que for caracterizado grave dano material ou de imagem ao STJ o qual impacte severamente as atividades finalísticas ou os serviços críticos mantidos pelo Tribunal;

IX – usuária ou usuário de TIC: qualquer pessoa física ou jurídica que utilize ou interaja com os ativos de TIC do STJ, sendo classificado em:

a) interno: magistrada, magistrado, servidora, servidor (ativa/o, aposentada/o, cedida/o ou licenciada/o), colaboradora, colaborador ou estagiária, estagiário que possua identificação na rede de dados do STJ;

b) externo: cidadã, cidadão, advogada, advogado, fornecedora, fornecedor ou prestadora, prestador de serviço;

c) instituição: ente público ou privado, compreendendo os órgãos da administração pública direta (indireta, sociedades, empresas privadas ou mistas);

d) instituição integrada: usuárias ou usuários de TIC pertencentes a instituições que possuam soluções tecnológicas integradas com o STJ.

Seção III

Dos Objetivos

Art. 3º São objetivos da gestão de vulnerabilidades cibernética de TIC:

I – estabelecer papéis e responsabilidades para gestoras e gestores de TIC e para as equipes que atuam na gestão, administração, identificação e correção de vulnerabilidades;

II – prevenir a exploração de vulnerabilidades técnicas nos ativos de TIC do STJ por intermédio de ações para a sua identificação, classificação e tratamento;

III – promover a capacidade de resiliência cibernética do STJ.

Seção IV

Da Gestão de Vulnerabilidades de Tecnologia da Informação e Comunicação

Art. 4º A gestão de vulnerabilidades de Tecnologia da Informação e Comunicação é um conjunto de atividades coordenadas e executadas de forma contínua que têm por objetivo a redução, a níveis aceitáveis de risco, das vulnerabilidades cibernéticas encontradas em um determinado ativo, conjunto de ativos ou ambiente computacional.

Art. 5º O processo de gestão de vulnerabilidades de Tecnologia da Informação e Comunicação contempla:

I – atualização contínua de repositório de referência a partir de listas públicas e privadas de vulnerabilidades cibernéticas, de forma a obter informações em tempo hábil para a realização das mitigações necessárias;

II – identificação das vulnerabilidades existentes dentro do ambiente tecnológico do STJ, bem como da interação com instituições integradas a partir do repositório de referência;

III – classificação e priorização das vulnerabilidades identificadas;

IV – tratamento das vulnerabilidades identificadas, consistindo na correção ou adoção de controles de acordo com os limites temporais necessários para cada tipo de vulnerabilidade definidos neste normativo, de modo a minimizar a probabilidade de exploração das vulnerabilidades;

V – comunicação das vulnerabilidades identificadas aos responsáveis e às partes interessadas.

Parágrafo único. A documentação atualizada do processo de gestão de vulnerabilidades cibernéticas será divulgada e publicada no portal de Processos de Tecnologia da Informação e Comunicação, na página da Secretaria de Tecnologia da Informação e Comunicação, na intranet.

Art. 6º O processo de gestão de vulnerabilidades cibernéticas deverá:

I – ser adequado para a capacidade operacional das equipes do STJ;

II – refletir as vulnerabilidades por tipo, de acordo com a seção responsável pela correção, respeitando a hierarquia organizacional da Secretaria de Tecnologia da Informação e Comunicação;

III – ser priorizado conforme os serviços críticos do STJ.

Art. 7º Considera-se pré-requisito para a realização do processo de gestão de vulnerabilidades cibernéticas a existência de um inventário completo e atualizado dos ativos de Tecnologia da Iinformação e Comunicação.

§ 1º O inventário deve identificar, no mínimo, todos os ativos de *hardware*, *software*, aplicações, serviços em nuvem, o grau de criticidade de cada ativo e a/o responsável pela sua gestão.

§ 2º Compete a cada coordenadoria da Secretaria de Tecnologia da Informação e Comunicação a atualização do inventário do ativo de TIC sob sua responsabilidade.

Art. 8º São fontes confiáveis para a atualização contínua do repositório de referência de vulnerabilidades:

I – vulnerabilidades divulgadas por fabricantes das soluções de TIC;

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

III – boletins de equipes governamentais de resposta a incidentes;

IV – fóruns e sites especializados.

Art. 9º Serão realizadas varreduras periódicas no parque tecnológico do STJ, de forma automatizada ou manual, para identificar as vulnerabilidades existentes.

§ 1º As varreduras de que trata o *caput* serão, preferencialmente, executadas utilizando credenciais autenticadas para permitir análises mais assertivas, havendo, ainda, a possibilidade da utilização de clientes instalados para casos específicos.

§ 2º Serão aplicadas, periodicamente, varreduras do tipo “reteste” ou varreduras de remediação, para fins de validação de vulnerabilidades e dos controles de segurança aplicados, assim como serão realizados testes de invasão controlados, para fins de validação dos controles de segurança aplicados.

Art. 10. As vulnerabilidades identificadas na varredura deverão ser registradas de forma centralizada e classificadas de acordo com, no mínimo, critérios estabelecidos por práticas e padrões de mercado aplicáveis ao contexto do Tribunal.

Art. 11. As vulnerabilidades serão classificadas de acordo com:

I – níveis de criticidade atribuídos aos itens do inventário de ativos, consoante indicado no art. 7º;

II – conformidade com o risco de exploração da vulnerabilidade;

III – classificação da vulnerabilidade.

Art. 12. A priorização do tratamento das vulnerabilidades será definida conforme a classificação numérica, variando de 0 a 10, como a seguir:

I – baixa: de 0 a 3,9;

II – média: de 4,0 a 6,9;

III – alta: de 7,0 a 8,9;

IV – crítica: de 9,0 a 10.

Art. 13. É ordem de priorização para vulnerabilidades de mesma classificação numérica:

I – tipo de sistema afetado;

II – exposição (interna ou externa);

III – dados sensíveis;

IV – *exploits* conhecidos;

V – histórico de ataques;

VI – capacidade de resposta (baixa, alta ou média).

Art. 14. As vulnerabilidades serão elencadas por tipos e entregues relatórios às áreas responsáveis para o devido tratamento, respeitando a ordem das estratégias a seguir:

I – evitar a exploração da vulnerabilidade (ex. corrigir ou atualizar);

II – reduzir o risco da exploração da vulnerabilidade (ex. mitigar);

III – compartilhar o risco da exploração da vulnerabilidade (ex. seguro);

IV – aceitar a vulnerabilidade.

Art. 15. Na ferramenta central de gestão de vulnerabilidades, deverá constar a lista de todas as vulnerabilidades identificadas e separadas por equipe responsável pelo tratamento, contendo a causa-raiz e a ação recomendada para a correção.

Art. 16. No 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 antes da aplicação em ambiente de produção;

III – as mudanças no ambiente motivadas pelas correções das vulnerabilidades que serão implantadas de acordo com o processo de gestão de mudanças, porém respeitando os prazos para tratamento atribuídos à vulnerabilidade.

Art. 17. Os relatórios e registros gerados durante a execução do processo de gestão de vulnerabilidades cibernéticas serão tratados e armazenados de forma segura e com acesso reservado às unidades envolvidas.

Seção V

Da Comunicação

Art. 18. 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 corrigidos em tempo aceitável;

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

III – proposição de melhorias nos processos da gestão de vulnerabilidades.

Art. 19. Deverá haver escalonamento na comunicação do relatório contendo as

vulnerabilidades identificadas quando o prazo de tratamento das vulnerabilidades pelas áreas for ultrapassado.

Parágrafo único. O escalonamento de que trata o *caput* se dará na seguinte ordem:

I – comunicação à área responsável pela aplicação das correções;

II – comunicação às coordenadorias e à/ao titular da Secretaria de Tecnologia da Informação e Comunicação a respeito da evolução dos riscos e dos achados das varreduras;

III – comunicação ao Comitê de Gestão de Riscos para os casos em que o tratamento das vulnerabilidades estiver em desacordo com a declaração de apetite de riscos do STJ.

Seção VI

Das Responsabilidades

Art. 20. Para assegurar a rastreabilidade adequada das vulnerabilidades, as responsabilidades são segregadas, observados os seguintes parâmetros:

I – Coordenadoria de Segurança da Informação e Defesa Cibernética – CSID: responsável pela execução das varreduras de segurança, classificação das vulnerabilidades, monitoramento das fontes de consulta confiáveis relacionadas a vulnerabilidades, acompanhamento do tratamento das vulnerabilidades e pela melhoria e atualização do processo de gestão de vulnerabilidades;

II – Coordenadoria de Infraestrutura – Ciep: responsável por aplicar tempestivamente as atualizações e correções de segurança em todo o parque tecnológico hospedado na nuvem e nos datacenters do STJ (ex. sistemas operacionais, equipamentos servidores, dispositivos de rede, *appliances*, serviços, *softwares*, bancos de dados etc.) e por acompanhar, mediante acesso regular à ferramenta central de análise de vulnerabilidades disponibilizada pela CSID, as vulnerabilidades identificadas de sua responsabilidade;

III – Coordenadoria de Relacionamento – Core: responsável por aplicar tempestivamente as atualizações e correções de segurança dos sistemas operacionais e *softwares* das estações de trabalho, *notebooks*, *tablets*, impressoras, balanceadores, ponto biométrico e quiosques no parque tecnológico do Tribunal e por acompanhar, mediante acesso regular à ferramenta central de análise de vulnerabilidades disponibilizada pela Coordenadoria de Segurança da Informação e Defesa Cibernética, as vulnerabilidades identificadas de sua responsabilidade;

IV – Coordenadoria de Desenvolvimento de Soluções de Software – CDES: responsável por aplicar, tempestivamente, as atualizações e correções de segurança referentes aos sistemas e serviços informatizados gerenciados por ela e por acompanhar, mediante acesso regular à ferramenta central de análise de vulnerabilidades disponibilizada pela Coordenadoria de Segurança da Informação e Defesa Cibernética, as vulnerabilidades identificadas em ativos de TIC de sua responsabilidade;

V – Coordenadoria de Tecnologia da Comunicação – CCOM: responsável por aplicar tempestivamente as atualizações e correções de segurança referentes aos equipamentos e serviços por eles gerenciados (ex. aparelhos IP, celulares, central telefônica, roteadores, *firewalls* etc.) e por acompanhar, mediante acesso regular à ferramenta central de análise de vulnerabilidades disponibilizada pela Coordenadoria de Segurança da Informação e Defesa Cibernética, as vulnerabilidades identificadas de sua responsabilidade;

VI – Comitê Gestor de Tecnologia da Informação e Comunicação – CGeTIC: definirá a área responsável pelo tratamento das vulnerabilidades dos ativos não contemplados na base de dados de

gerenciamento de configuração e a prioridade em que as vulnerabilidades serão tratadas nas situações em que ocorrer conflito de competência.

Seção VII

Das Disposições Finais

Art. 21. A revisão desta instrução normativa ocorrerá a cada três anos ou sempre que se fizer necessária ou conveniente para o STJ.

Art. 22. O descumprimento desta instrução normativa deverá ser imediatamente registrado como incidente de segurança da informação e reportado à Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação – Etir para apuração e consequente adoção das providências cabíveis.

Art. 23. Em casos excepcionais ou de risco iminente aos ativos de Tecnologia da Informação e Comunicação (ex. vulnerabilidades críticas e exploração de dia zero), a/o titular da Secretaria de Tecnologia da Informação e Comunicação poderá autorizar a distribuição e implementação de atualizações tempestivas e sem prévio aviso.

Art. 24. Os casos omissos serão resolvidos pelo Comitê Gestor de Tecnologia da Informação e Comunicação.

Art. 25. Esta instrução normativa entra em vigor na data de sua publicação.

SERGIO JOSÉ AMERICO PEDREIRA

Documento assinado eletronicamente por **Sergio José Americo Pedreira**, **Diretor-Geral**, em 18/11/2024, às 15:14, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.stj.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **5907060** e o código CRC **CFF6357E**.
