SUPERINTENDÊNCIA DE SEGUROS PRIVADOS

RESOLUÇÃO SUSEP Nº 89, DE 21 DE JULHO DE 2026

Institui a Política de Gestão de Vulnerabilidades de Tecnologia da Informação no âmbito da Susep.

O SUPERINTENDENTE DA SUPERINTENDÊNCIA DE SEGUROS PRIVADOS – SUSEP, torna público que Conselho Diretor desta Autarquia, em reunião ordinária realizada em 15 de julho de 2026, no uso das atribuições que lhe conferem o inciso VI do Art. 8º do Regimento Interno, aprovado pela Resolução CNSP nº 490, de 12 de março de 2026, tendo em vista o disposto na Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025, na Resolução Susep nº 45, de 17 de outubro de 2024, e na Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, bem como o que consta do Processo Susep nº 15414.666235/2025-31,

R E S O L V E :

Art. 1º Fica instituída a Política de Gestão de Vulnerabilidades de Tecnologia da Informação - PGVTI no âmbito da Susep, nos termos desta Resolução.

Art. 2º A PGVTI tem por objetivo estabelecer diretrizes, processos e responsabilidades para a identificação, avaliação, priorização, tratamento e comunicação de vulnerabilidades em ativos de tecnologia da informação - TI da Susep.

Parágrafo único. O processo de que trata o *caput* deverá ser contínuo e estruturado, incluindo o mapeamento dos ativos de TI, de suas vulnerabilidades e das medidas de tratamento cabíveis.

Art. 3º A PGVTI se aplica a todos os ativos de TI da Susep, exceto os que:

I - não possuam capacidade técnica para realização de análises de vulnerabilidade de TI;

II - estejam sujeitos a restrições contratuais ou normativas que impeçam a execução dessas análises;

III - sejam considerados tecnicamente inviáveis para fins de gestão de vulnerabilidades de TI, mediante justificativa técnica da área responsável pelo ativo, devidamente fundamentada, e manifestação da área responsável pela segurança da informação.

IV - As exceções de que trata este artigo deverão ser formalmente justificadas pela unidade responsável pelo ativo de TI, com manifestação da área de segurança da informação, e submetidas à aprovação do Gestor de Segurança da Informação.

Art. 4º Para os fins desta Política, aplicam-se as definições constantes do Glossário de Segurança da Informação, instituído pela Portaria GSI/PR nº 93, de 18 de outubro de 2021, e da Política de Segurança da Informação da Susep - POSIN, além das seguintes:

I - Ativos de TI: termo que engloba sistemas operacionais, softwares, APIs, infraestrutura de redes, servidores, computadores, bancos de dados, sistemas de informação, aplicações e serviços de TI;

II - Gestão de vulnerabilidades de TI: processo contínuo de identificação, avaliação, documentação, tratamento, comunicação e remediação de vulnerabilidades;

III - Patch: uma parte de código adicional desenvolvido para corrigir falhas ou problemas em um software existente;

IV - Remediação: ação que resulta na eliminação da vulnerabilidade no ativo de TI em que foi identificada;

V - Mitigação: atividade que resulta na redução da probabilidade de exploração de uma vulnerabilidade identificada ou na redução do impacto, caso seja explorada;

VI - Tratamento: compreende a remediação e a mitigação de vulnerabilidades de TI.

Art. 5º Esta política observa os seguintes princípios:

I - proteção da confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade das informações sob responsabilidade da Susep;

II - alinhamento à Política de Segurança da Informação da Susep - POSIN; e

III - conformidade com os dispositivos legais, infralegais e com as melhores práticas aplicáveis em gestão de vulnerabilidades de TI.

Art. 6º O processo de gestão de vulnerabilidades de TI é cíclico e compreende as seguintes etapas:

I - mapeamento de ativos;

II - identificação de vulnerabilidades de TI;

III - avaliação das vulnerabilidades de TI;

IV - priorização das vulnerabilidades de TI;

V - tratamento das vulnerabilidades de TI; e

VI - comunicação dos resultados das ações do ciclo de gestão de vulnerabilidades de TI.

§ 1º O processo de gestão de vulnerabilidades de TI deverá ser estabelecido, documentado e revisto periodicamente, ou sempre que necessário, mediante proposta da área responsável pela segurança da informação, em articulação com as unidades de TI, a ser submetida à aprovação do Gestor de Segurança da Informação.

§ 2º A consistência e a eficácia do processo de gestão de vulnerabilidades deverão ser avaliadas por meio de indicadores e métricas definidos pelo Gestor de Segurança da Informação, em conjunto com a área de segurança da informação.

§ 3º As atividades do ciclo de gestão de vulnerabilidades de TI deverão ser desempenhadas com auxílio de fontes externas de dados de vulnerabilidades de TI, como sites de segurança da informação, ferramentas de inteligência em ameaças e vulnerabilidades (por exemplo, MISP), boletins de segurança ou publicações de fornecedores de software ou hardware, que indiquem vulnerabilidades de TI conhecidas e suas respectivas medidas de remediação.

Art. 7º O ciclo de gerenciamento de vulnerabilidades de TI compreende o registro dos ativos de TI a serem analisados para identificação de vulnerabilidades.

§ 1º A área responsável por operacionalizar as ações de segurança da informação manterá o mapeamento dos ativos de TI a que se refere o *caput.*

§ 2º Caberá à área responsável pela segurança da informação definir os itens e as características a serem registrados no mapeamento dos ativos de TI, inclusive os campos obrigatórios e facultativos, conforme sua categoria e criticidade.

§ 3º Todas as unidades de TI deverão colaborar com o fornecimento dos dados necessários à manutenção do mapeamento de ativos de TI.

§ 4º O mapeamento de ativos de TI deverá ser mantido atualizado sempre que houver mudanças no ambiente de TI da Susep.

Art. 8º As vulnerabilidades existentes nos ativos de TI mapeados deverão ser identificadas.

§ 1º Deverão ser utilizadas preferencialmente ferramentas automatizadas para varredura de vulnerabilidades nos recursos de TI.

§ 2º As vulnerabilidades de TI identificadas deverão ser detalhadas e registradas em banco de dados centralizado.

§ 3º Não serão objeto de atividades de identificação de vulnerabilidades os ativos de TI que se enquadrarem nas exceções previstas no art. 3º.

§ 4º Poderão ser realizados testes de invasão ou penetração - Pentest para fornecimento de informações mais precisas e relevantes sobre as vulnerabilidades atuais do ambiente de TI da Susep, observadas as salvaguardas necessárias à preservação do funcionamento do ambiente.

§ 5º As vulnerabilidades de TI identificadas deverão ser confirmadas previamente à sua comunicação, sempre que tecnicamente viável, de modo a preservar a credibilidade das atividades de gerenciamento de vulnerabilidades.

§ 6º As ferramentas de varredura de vulnerabilidades de TI deverão ser ajustadascontinuamente com vistas a evitar erros (falsos positivos e falsos negativos) no mapeamento por elas realizado.

§ 7º As ferramentas automatizadas a que se refere o §1º do *caput* serão selecionadas e implantadas no ambiente da Susep pela área responsável pela segurança da informação.

Art. 9º As vulnerabilidades de TI identificadas deverão ser avaliadas e classificadas com base na gravidade, alcance e risco que representam para a Susep.

§ 1º As vulnerabilidades de TI classificadas serão ordenadas segundo fatores como gravidade, criticidade do sistema afetado, facilidade de exploração e disponibilidade de solução.

§ 2º A lista ordenada de vulnerabilidades de TI será a base do planejamento de remediação e mitigação de vulnerabilidades de TI.

Art. 10. A remediação e a mitigação de vulnerabilidades de TI compreendem a aplicação de correções, atualizações, patches de segurança ou outras contramedidas destinadas a eliminar ou reduzir vulnerabilidades identificadas.

§ 1º A área de segurança da informação definirá o plano de tratamento das vulnerabilidades avaliadas, em articulação com a unidade responsável pelo ativo de TI afetado, tendo por base a criticidade das vulnerabilidades e a disponibilidade de solução e de recursos para sua aplicação.

§ 2º O tratamento de vulnerabilidades de TI poderá ser realizado inicialmente em ambiente de homologação e, quando cabível, posteriormente em ambiente de produção, conforme decisão conjunta da unidade responsável pelo ativo de TI afetado e da área responsável pela segurança da informação, observadas as diretrizes desta última.

§ 3º O tratamento de vulnerabilidades de TI deverá observar o disposto no normativo interno que disciplina o processo de mudanças em ambientes computacionais.

§ 4º A unidade responsável pelo ativo de TI afetado, assim considerada aquela formalmente designada como responsável por sua gestão no âmbito institucional, deverá coordenar o tratamento da vulnerabilidade, competindo-lhe promover a implementação das ações previstas no plano de tratamento, ainda que com o apoio de outras unidades, bem como coletar e manter evidências que comprovem sua execução.

§ 5º A área de segurança da informação compilará as vulnerabilidades que persistirem após o respectivo tratamento, com a devida justificativa técnica, submetendo-as ao Comitê de Segurança da Informação (CSI) para análise e deliberação quanto às vulnerabilidades remanescentes e aos riscos associados.

Art. 11. Os resultados das atividades do ciclo de gerenciamento de vulnerabilidades de TI deverão ser periodicamente consolidados e comunicados.

§ 1º A área de segurança da informação realizará a consolidação periódica das atividades do ciclo de gestão de vulnerabilidades de TI, observado, no mínimo, intervalo trimestral.

§ 2º Deverão ser informados dos resultados das atividades do ciclo de gestão de vulnerabilidades de TI:

I - o Comitê de Segurança da Informação - CSI; e

II - as unidades de Tecnologia da Informação.

§ 3º Os dados da consolidação serão objeto de norma complementar.

Art. 12. Compete às unidades de TI da Susep:

I - operacionalizar as ações necessárias ao mapeamento, identificação, avaliação e tratamento das vulnerabilidades nos ativos de TI sob sua responsabilidade;

II - manter atualizado o mapeamento dos ativos de TI sob sua responsabilidade, incluindo características técnicas, criticidade e dependências, para fins de apoio ao ciclo de gestão de vulnerabilidades de TI;

III - participar da execução, quando aplicável, das atividades de remediação e mitigação, observadas as diretrizes da área de segurança da informação e o normativo interno de gestão de mudanças em ambientes computacionais;

IV - colaborar com a área responsável pela segurança da informação na disponibilização de informações, evidências e pareceres técnicos necessários à execução do processo de gestão de vulnerabilidades de TI; e

V - comunicar tempestivamente à área de segurança da informação quaisquer limitações técnicas, riscos residuais, inviabilidades ou impactos que possam afetar as atividades de gestão de vulnerabilidades de TI.

Art. 13. Compete ao Gestor de Segurança da Informação:

I - coordenar a elaboração, revisão e atualização desta Política e dos normativos e procedimentos complementares;

II - acompanhar a implantação e a execução das ações previstas nesta Política;

III - promover a cultura de gestão de vulnerabilidades de TI; e

IV - articular a disponibilização de recursos essenciais à implementação das ações de gestão de vulnerabilidades de TI.

Art. 14. Compete ao Comitê de Segurança da Informação - CSI:

I - deliberar sobre as propostas de instituição e de alteração da PGVTI, para encaminhamento às instâncias competentes;

II - acompanhar e avaliar, em nível estratégico, a implementação das ações de gestão de vulnerabilidades de TI no âmbito da Susep; e

III - analisar, com base em justificativa técnica, e deliberar quanto às vulnerabilidades remanescentes e aos riscos associados.

Art. 15. Compete à área responsável pela segurança da informação:

I - implantar, configurar, operar e monitorar a estrutura de gestão de vulnerabilidades de TI;

II - propor, implementar e manter procedimentos operacionais de gestão de vulnerabilidades de TI, em conformidade com esta Política e com as diretrizes do Gestor de Segurança da Informação;

III - receber, analisar e responder às notificações e às demandas relacionadas à gestão de vulnerabilidades de TI;

IV - apoiar tecnicamente a avaliação, priorização e tratamento das vulnerabilidades de TI identificadas, em conjunto com as unidades de TI;

V - executar, juntamente com as unidades de TI, as atividades de tratamento das vulnerabilidades de TI;

VI - atualizar os indicadores e métricas do processo de gestão de vulnerabilidades de TI;

VII - apoiar o Gestor de Segurança da Informação na elaboração, revisão e atualização da PGVTI e de normas internas complementares;

VIII - pesquisar, propor, apoiar contratações, implantar e manter soluções técnicas para gestão de vulnerabilidades de TI no âmbito da Susep; e

IX - analisar, consolidar e comunicar os resultados das atividades relacionadas à gestão de vulnerabilidades de TI.

Art. 16. As regras, medidas, controles e procedimentos operacionais de gestão de vulnerabilidades de TI poderão ser detalhados em normas internas e procedimentos complementares elaborados pela área responsável pela segurança da informação.

Art. 17. As atividades de gestão de vulnerabilidades previstas nesta PGVTI deverão ser implementadas de forma gradual, observado o prazo máximo de vinte e quatro meses, contado da data de sua publicação, sob coordenação da área responsável pela segurança da informação.

Art. 18. Esta Resolução entra em vigor na data de sua publicação.

Documento assinado eletronicamente por **ALESSANDRO SERAFIN OCTAVIANI LUIS (MATRÍCULA 1860655)**, **Superintendente da Susep**, em 29/07/2026, às 18:50, conforme horário oficial de Brasília, de acordo com o art. 6º do Decreto nº 8.539/2015.

A autenticidade do documento pode ser conferida no site https://sei.susep.gov.br/sei/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2839217** e o código CRC **75CDC81B**.

Referência: Processo nº 15414.666235/2025-31 SEI nº 2839217