Modelo de Norma de Gestão de Vulnerabilidades

Programa de Privacidade e Segurança da Informação

PPSI 2.0

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Versão 1.0

Brasília, 13 de maio de 2026

MODELO DE NORMA DE GESTÃO DE VULNERABILIDADES

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS
Esther Dweck
Ministra

SECRETARIA DE GOVERNO DIGITAL
Rogério Souza Mascarenhas
Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO
Leonardo Rodrigo Ferreira
Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PRIVACIDADE
Marta Juvina de Medeiros
Coordenadora-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO
Loriza Andrade Vaz de Melo
Coordenadora-Geral de Segurança da Informação

EQUIPE TÉCNICA DE ELABORAÇÃO
Anderson Souza de Araújo
Ricardo Borges Almeida

EQUIPE DE REVISÃO
Marta Juvina de Medeiros

Histórico de versões

Data	Versão	Descrição	Autor
13/05/2026	1.0	Elaboração do Modelo de Norma de Gestão de Vulnerabilidades (PPSI 2.0)	Equipe Técnica de Elaboração

Orientações

Esta seção consigna informações básicas para a elaboração da Norma de Gestão de Vulnerabilidades do órgão ou entidade:

1. este modelo, assim como todos os modelos disponibilizados pela Diretoria de Privacidade e Segurança da Informação (DEPSI) no âmbito do Programa de Privacidade e Segurança da Informação (PPSI) – instituído pela Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025 –, serve como referência para órgãos e entidades do SISP. Seu uso exige análise e adaptação (com inclusão ou exclusão de diretrizes) para atender às particularidades locais, alinhando-se à realidade específica e às boas práticas;
2. o presente documento apoia diretamente a implementação dos controles 7 e 16 do *framework* do PPSI 2.0;
3. as informações [destacadas em amarelo] neste modelo devem ser substituídas conforme o caso concreto. As [dispostas em vermelho], por sua vez, devem ser removidas. Também devem ser removidas, antes da publicação da norma, a capa, esta página e a página final.

Licença *Creative Commons*

[1] Disponível em: https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.

[ATO NORMATIVO Nº XX, DE XX DE XXXXXXXXX DE 20XX)

Dispõe sobre a Norma de Gestão de Vulnerabilidades no âmbito do [órgão ou entidade].

O [representante do órgão ou entidade], no uso da atribuição que lhe confere o [dispositivo legal], e tendo em vista o disposto na Lei nº 13.709, de 14 de agosto de 2018, no Decreto nº 11.856, de 26 de dezembro de 2023, e no Decreto nº 12.572, de 4 de agosto de 2025, resolve:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Norma de Gestão de Vulnerabilidades do [órgão ou entidade], em complemento à Política de Gestão de Vulnerabilidades.

Art. 2º Esta Norma constitui um dos instrumentos de implementação do Programa de Privacidade e Segurança da Informação (PPSI) disposto na Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025.

[listar outras diretrizes que julgar necessário]

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 3º Os termos e definições desta Norma observam o disposto na Lei nº 13.709, de 14 de agosto de 2018 (LGPD), e no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República, aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021, além de:

I - gestão de vulnerabilidades: processo sistemático de identificar, avaliar, tratar e monitorar vulnerabilidades em ativos de informação; e

II - varredura de vulnerabilidades: processo automatizado de identificação de vulnerabilidades em ativos de informação.

[acrescentar demais conceitos e definições empregados neste documento]

CAPÍTULO III

DA FINALIDADE

Art. 4º Esta Norma tem por finalidade estabelecer os critérios operacionais e requisitos necessários à implementação das diretrizes previstas na Política de Gestão de Vulnerabilidades.

[listar outros objetivos que julgar necessário]

CAPÍTULO IV

DO PROCESSO DE GESTÃO DE VULNERABILIDADES

Art. 5º O processo de gestão de vulnerabilidades deve abranger todo o ciclo de vida dos ativos de informação e considerar, no mínimo:

I - a identificação e a detecção de vulnerabilidades;

II - a avaliação e a priorização com base em risco, incluindo análise do impacto institucional e a criticidade dos ativos envolvidos;

III - o tratamento;

IV - a validação da efetividade das correções;

V - o monitoramento contínuo por meio de métricas formais para medir a eficiência e a consistência do processo;

VI - a produção de relatórios periódicos e sob demanda; e

VII - a definição de funções e responsabilidades das equipes envolvidas em cada uma das etapas.

Art. 6º A gestão de vulnerabilidades em serviços de terceiros deve considerar:

I - a definição formal de responsabilidades;

II - os requisitos contratuais de segurança; e

III - os mecanismos de acompanhamento e verificação.

[listar outras diretrizes que julgar necessário]

CAPÍTULO V

DA IDENTIFICAÇÃO DE VULNERABILIDADES

Art. 7º A identificação de vulnerabilidades consiste no levantamento sistemático das fraquezas e falhas de segurança da informação presentes nos ativos de informação, com o objetivo de subsidiar as etapas subsequentes de avaliação e tratamento.

Art. 8º A identificação de vulnerabilidades observa os seguintes requisitos:

I - a definição prévia do escopo das varreduras;

II - a utilização de ferramentas configuradas e atualizadas;

III - a execução periódica de varreduras e testes conforme criticidade dos ativos;

IV - a complementação por técnicas manuais, quando aplicável; e

V - a revisão periódica dos métodos e ferramentas utilizadas.

[listar outras diretrizes que julgar necessário]

CAPÍTULO VI

DA AVALIAÇÃO DE VULNERABILIDADES

Art. 9º A avaliação de vulnerabilidades consiste na análise dos resultados obtidos na etapa de identificação, com o objetivo de subsidiar a priorização e o tratamento adequado das vulnerabilidades.

Art. 10. A etapa de avaliação das vulnerabilidades compreende, no mínimo:

I - a validação dos resultados identificados, com a consequente eliminação de falsos positivos;

II - a classificação quanto à severidade das vulnerabilidades, com base em modelo institucional ou referências reconhecidas; e

III - a priorização para o tratamento das vulnerabilidades, considerando risco, criticidade dos ativos e impacto institucional.

Art. 11. Os resultados da avaliação devem ser registrados de forma estruturada e rastreável, de modo a subsidiar o processo de tratamento das vulnerabilidades.

[listar outras diretrizes que julgar necessário]

CAPÍTULO VII

DO TRATAMENTO DE VULNERABILIDADES

Art. 12. O tratamento das vulnerabilidades compreende:

I - a correção;

II - a mitigação; e

III - a aceitação do risco, quando aplicável.

Art. 13. A aplicação das correções deve observar:

I - a validação prévia, sempre que possível;

II - a utilização de fontes confiáveis;

III - o registro das ações realizadas; e

IV - a integração com o processo de gestão de mudanças.

Art. 14. As vulnerabilidades não tratadas no prazo definido devem ser submetidas a processo formal de exceção.

[listar outras diretrizes que julgar necessário]

CAPÍTULO VIII

DA VERIFICAÇÃO DE VULNERABILIDADES

Art. 15. A verificação de vulnerabilidades consiste na confirmação da efetividade das ações de tratamento realizadas, com o objetivo de assegurar que as vulnerabilidades foram adequadamente remediadas antes do encerramento do processo.

Art. 16. As ações de tratamento de vulnerabilidades devem ser submetidas à verificação para confirmação da remediação.

Art. 17. A verificação para confirmação da remediação deve considerar, no mínimo:

I - a reexecução de varreduras;

II - a validação técnica das correções; e

III - a análise de evidências.

[listar outras diretrizes que julgar necessário]

CAPÍTULO IX

DO REGISTRO DE VULNERABILIDADES

Art. 18. O registro de vulnerabilidades consiste no conjunto de informações estruturadas que documenta o ciclo de vida de cada vulnerabilidade identificada, desde a detecção até o encerramento, com o objetivo de assegurar rastreabilidade, subsidiar o monitoramento e apoiar a prestação de contas institucional.

Art. 19. O registro de vulnerabilidades deve conter, no mínimo:

I - a identificação da vulnerabilidade;

II - o ativo afetado;

III - a classificação de severidade;

IV - a origem da identificação;

V - o status do tratamento;

VI - o responsável; e

VII - os prazos definidos.

Art. 20. O registro de vulnerabilidades integra-se, sempre que possível, às demais ferramentas institucionais de gestão e monitoramento.

[listar outras diretrizes que julgar necessário]

CAPÍTULO X

DO MONITORAMENTO E RELATÓRIOS DE VULNERABILIDADES

Art. 21. O monitoramento do processo de gestão de vulnerabilidades consiste no acompanhamento contínuo dos indicadores de desempenho, das tendências de ocorrência e da eficácia das ações de

tratamento, com o objetivo de detectar desvios, apoiar a tomada de decisão e promover a melhoria contínua do processo.

Art. 22. O processo de gestão de vulnerabilidades deve ser monitorado por meio de registros e indicadores institucionais.

Art. 23. Devem ser elaborados relatórios periódicos contendo, no mínimo:

I - as vulnerabilidades identificadas;

II - o status do tratamento;

III - os níveis de risco; e

IV - as tendências e recorrências.

[listar outras diretrizes que julgar necessário]

CAPÍTULO XI

DISPOSIÇÕES FINAIS

Art. 24. Esta Norma deve ser revisada e atualizada periodicamente a cada [2 (dois)] anos ou quando eventos ou mudanças significativas assim o exigirem.

Art. 25. O descumprimento das disposições desta Norma sujeitará o infrator às sanções administrativas, disciplinares, contratuais ou legais cabíveis, aplicadas conforme a legislação vigente.

Art. 26. Quaisquer exceções a esta Norma devem ser integralmente documentadas e submetidas à aprovação do [comitê de segurança da informação ou estrutura equivalente], com justificativa técnica e prazo de correção definido.

Art. 27. Esta Norma entra em vigor na data de sua publicação.

[listar outras disposições finais que julgar necessário]

gov.br

Dúvida?

Entre em contato conosco

Acesse o sítio do PPSI 2.0:
PPSI 2.0 - Governo Digital