Modelo de Política de Gestão de Vulnerabilidades

MINISTÉRIO DA
GESTÃO E DA
INOVAÇÃO EM
SERVIÇOS PÚBLICOS

Programa de Privacidade e Segurança da Informação
PPSI 2.0

Versão 1.0

Brasília, 13 de maio de 2026

MODELO DE POLÍTICA 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 Política de Gestão de Vulnerabilidades (PPSI 2.0)	Equipe Técnica de Elaboração

Orientações

Esta seção consigna informações básicas para a elaboração da Política 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 política, 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 Política 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 PRELIMINARES

Art. 1º Fica instituída a Política de Gestão de Vulnerabilidades do [órgão ou entidade].

Art. 2º Esta Política dispõe sobre as diretrizes para a gestão de vulnerabilidades de segurança da informação.

Art. 3º Esta Política 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. 4º Os termos e definições desta Política 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.

[acrescentar demais conceitos e definições empregados neste documento]

CAPÍTULO III

DA FINALIDADE

Art. 5º Esta Política tem por objetivo:

I - assegurar a identificação, avaliação, tratamento e monitoramento contínuo de vulnerabilidades, empregando uma abordagem sistemática proativa baseada em risco;

II - reduzir a exposição a riscos de segurança da informação; e

III - proteger os ativos de informação quanto à confidencialidade, integridade e disponibilidade.

[listar outros objetivos que julgar necessário]

CAPÍTULO IV

DO ESCOPO

Art. 6º Esta Política abrange todos os ativos de informação gerenciados pela organização, sejam esses de sua propriedade ou custodiados pela organização.

Art. 7º Esta Política aplica-se a todos os agentes públicos, colaboradores, contratados e terceiros e demais partes relacionadas com o processo de gestão de vulnerabilidades da organização.

[acrescentar demais definições sobre o escopo]

CAPÍTULO V

DAS DIRETRIZES

Art. 8º A organização deve elaborar, implementar e manter um processo formal, documentado e contínuo de gestão de vulnerabilidades.

Art. 9º O processo de gestão de vulnerabilidades deve utilizar, como referência primária, o inventário de ativos de informação mantido nos termos da Política de Gestão de Ativos de Informação.

Art. 10. A eficácia e a efetividade do processo de gestão de vulnerabilidades devem ser avaliadas de forma contínua, por meio da utilização de indicadores de desempenho, objetivando promover a melhoria contínua do processo.

Art. 11. A organização deve assegurar o registro centralizado e rastreável das vulnerabilidades identificadas.

Art. 12. As informações sobre vulnerabilidades devem ser comunicadas de forma tempestiva às partes interessadas, observados os critérios institucionais de confidencialidade.

Art. 13. A gestão de vulnerabilidades envolvendo terceiros deverá observar a definição formal de responsabilidades entre a organização e os respectivos prestadores de serviços.

[listar outras diretrizes que julgar necessário]

CAPÍTULO VI

DAS RESPONSABILIDADES

Art. 14. Compete ao agente público responsável pela gestão dos ativos de informação contribuir para o processo de gestão de vulnerabilidades, em conformidade com a Política de Gestão de Ativos de Informação e demais normativos aplicáveis.

Art. 15. Compete ao [comitê de segurança da informação ou estrutura equivalente]:

I - assessorar o gestor de segurança da informação e a alta administração na viabilização da implementação desta Política;

II - definir métricas e indicadores que permitam o acompanhando pelo próprio [comitê de segurança da informação ou estrutura equivalente] do desempenho do processo de gestão de vulnerabilidades; e

III - deliberar sobre situações relevantes, incluindo riscos elevados e exceções.

Art. 16. Compete à unidade gestora de tecnologia da informação:

I - implementar ações necessárias para apoiar o processo de gestão de vulnerabilidades técnicas;

II - manter registros das vulnerabilidades técnicas identificadas e das ações realizadas, incluindo tomadas de decisões; e

III - implementar métricas e indicadores de desempenho que permitam avaliar a eficácia do processo de gestão de vulnerabilidades técnicas.

Art. 17. Compete às unidades organizacionais:

I - apoiar a identificação da criticidade dos ativos de informação;

II - participar da priorização do tratamento das vulnerabilidades; e

III - apoiar a implementação de ações corretivas nos ativos sob sua responsabilidade.

Art. 18. Compete aos agentes públicos e demais usuários dos ativos de informação:

I - utilizar os ativos de informação em conformidade com as normas institucionais;

II - comunicar vulnerabilidades ou incidentes de segurança identificados; e

III - colaborar com as ações de tratamento de vulnerabilidades quando aplicável.

Art. 19. Compete às equipes responsáveis pela gestão de vulnerabilidades e pela gestão de ativos manter integração contínua entre seus processos e sistemas de controle, de modo que as informações sobre alterações, inclusões ou exclusões de ativos sejam refletidas tempestivamente no processo de gestão de vulnerabilidades.

[listar outros papéis e responsabilidades que julgar necessário]

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 20. Esta Política deve ser revisada e atualizada periodicamente a cada [3 (três)] anos ou quando eventos ou mudanças significativas assim o exigirem.

Art. 21. O descumprimento das disposições desta Política sujeitará o infrator às sanções administrativas, disciplinares, contratuais ou legais cabíveis, aplicadas conforme a legislação vigente.

Art. 22. Quaisquer exceções a esta Política deverão ser integralmente documentadas e submetidas à aprovação do [comitê de segurança da informação ou estrutura equivalente], observando:

I - a documentação da justificativa técnica, legal, normativa ou contratual;

II - a avaliação da área responsável e a aprovação por autoridade competente; e

III - o registro em processo de gerenciamento de exceções contendo prazo de validade, controles compensatórios, revisão periódica e avaliação de risco.

Art. 23. Esta Política 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