gov.br

Modelo de Política de Segurança da Informação

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 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

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
Adriano de Andrade Moura
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 Modelo de Política de Segurança da Informação (PPSI 2.0)	Equipe Técnica de Elaboração

Orientações

Esta seção consigna informações básicas para a elaboração da Política de Segurança da Informação 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 da medida 0.11 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 XXXXXXX DE 20XX)

Dispõe sobre a Política de Segurança da Informação no âmbito do [órgão ou entidade].

O [autoridade máxima 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, no Decreto nº 12.572, de 4 de agosto de 2025, e no art. 9º da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, resolve:

[acrescentar outros dispositivos legais que julgar necessário]

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Política de Segurança da Informação do [órgão ou entidade].

Art. 2º Esta Política dispõe sobre os princípios, as diretrizes, as responsabilidades e os mecanismos de gestão aplicáveis para promover a segurança da informação na organização.

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.

[acrescentar outras disposições gerais 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), nas normas editadas pela Agência Nacional de Proteção de Dados (ANPD) 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:

[acrescentar conceitos e definições empregados neste documento]

CAPÍTULO III

DA FINALIDADE

Art. 5º Esta Política tem por objetivo:

I - proteger os ativos de informação de propriedade ou custodiados pela organização;

II - preservar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

III - contribuir para a gestão eficiente dos riscos de segurança da informação; e

IV - assegurar a continuidade dos processos e serviços essenciais ao funcionamento da organização.

[listar outros objetivos que julgar necessário]

CAPÍTULO IV

DO ESCOPO

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

Art. 7º Esta Política aplica-se a todos os agentes públicos, colaboradores, contratados e terceiros que utilizem ou gerenciem ativos de informação em nome da organização.

[acrescentar demais definições sobre o escopo]

CAPÍTULO V

DOS PRINCÍPIOS

Art. 8º As atividades de segurança da informação devem observar os princípios constitucionais e administrativos que regem a Administração Pública Federal.

Art. 9º As iniciativas de segurança da informação devem estar vinculadas aos objetivos estratégicos, às competências legais e à finalidade institucional da organização.

Art. 10. As ações de segurança da informação devem ser conduzidas de forma colaborativa entre as unidades, cabendo a cada uma contribuir, no âmbito de suas competências, para o cumprimento das obrigações da organização, respeitadas suas especificidades e autonomia.

Art. 11. As medidas de segurança da informação devem preservar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações em todo o ciclo de vida dos ativos de informação.

Art. 12. As medidas de segurança da informação devem ser adotadas proporcionalmente à criticidade dos ativos de informação, às operações realizadas e à magnitude dos potenciais danos à organização e aos titulares de dados pessoais, no âmbito do processo institucional de gestão de riscos.

Art. 13. As ações de segurança da informação devem estar integradas à proteção de dados pessoais, observada a Política de Proteção de Dados Pessoais e normas dela decorrentes.

Art. 14. A segurança da informação deve abranger todo o ciclo de vida dos ativos de informação, desde a sua concepção até o descarte.

[listar outros princípios que julgar necessário]

CAPÍTULO VI

DAS DIRETRIZES

Art. 15. Toda informação produzida, recebida, custodiada ou tratada pela organização constitui ativo de informação e deve ser protegida nos termos desta Política e das normas dela decorrentes.

Art. 16. Os acessos aos ativos de informação devem observar o princípio do menor privilégio e a segregação de funções.

Art. 17. Devem ser elaborados políticas, normas, procedimentos e orientações relacionados à segurança da informação, abordando, no mínimo, os seguintes aspectos:

I - o uso aceitável dos ativos de informação;

II - o treinamento e a capacitação sobre a temática de segurança da informação, observado o disposto no Plano de Desenvolvimento de Pessoas;

III - as ações de conscientização sobre segurança da informação;

IV - a gestão de ativos de informação;

V - a gestão de mudanças em ativos de informação;

VI - o controle de acesso lógico e físico aos ativos de informação;

VII - a gestão de vulnerabilidades;

VIII - as defesas contra códigos maliciosos;

IX - a realização e a proteção de cópias de segurança (*backup*);

X - a gestão de incidentes de segurança da informação;

XI - a gestão de continuidade de negócios;

XII - a gestão de riscos de segurança da informação; e

XIII - a auditoria e a verificação de conformidade.

Art. 18. Deve ser instituído comitê ou estrutura equivalente para tratar das ações de segurança da informação, observada a composição mínima estabelecida no art. 21 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, acrescida do:

I - representante da alta administração, podendo ser atendido pelo representante de que trata o inciso II do art. 21 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020;

II - Encarregado pelo tratamento de dados pessoais;

III - responsável setorial pela gestão da integridade; e

IV - representante da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

Art. 19. Os contratos, convênios, acordos e instrumentos congêneres de prestação de serviços firmados pela organização que envolvam ativos de informação devem conter cláusulas específicas sobre requisitos de segurança proporcionais à criticidade dos ativos.

Art. 20. O investimento necessário em medidas de segurança da informação deve ser dimensionado conforme critérios de avaliação de risco, em alinhamento com o processo institucional de gestão de riscos.

[listar outras diretrizes gerais que julgar necessário]

CAPÍTULO VII

DAS RESPONSABILIDADES

Art. 21. Em adição às competências estabelecidas para a estrutura de governança do PPSI pela Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025, e pela legislação vigente, compete:

I - à alta administração:

a) instituir o comitê de segurança da informação ou estrutura equivalente;

b) instituir e implementar a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) no âmbito da organização [aplicável para as organizações que possuem competência formal e atribuição para administrar sua infraestrutura de rede de computadores, conforme NC nº 05/IN01/DSIC/GSIPR. Caso não seja a hipótese da sua organização, remover esta alínea.];

c) designar o Gestor de Segurança da Informação, e respectivo substituto, em ato administrativo próprio, de acordo com a legislação vigente;

d) fornecer os recursos necessários para assegurar o desenvolvimento e a implementação das medidas de segurança da informação; e

e) tratar as ações e decisões de segurança da informação em nível de relevância e prioridade adequados.

[listar outras atribuições que julgar necessário]

II - ao Encarregado pelo tratamento de dados pessoais atuar de forma articulada com o Gestor de Segurança da Informação no estabelecimento de medidas que envolvam, simultaneamente, segurança da informação e proteção de dados pessoais.

[listar outras atribuições que julgar necessário]

Art. 22. Compete ao comitê de segurança da informação ou estrutura equivalente, além do disposto no art. 20 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020:

I - participar da elaboração, formalização e aprovação do Programa de Governança em Segurança da Informação (PGSI), além de acompanhar sua implementação;

II - deliberar sobre exceções a esta Política e às normas de segurança da informação; e

III - promover a integração das ações de segurança da informação com as ações de proteção de dados pessoais e com a gestão da integridade institucional.

[listar outras atribuições que julgar necessário]

Parágrafo único. A composição, a estrutura, os recursos e o funcionamento do comitê de segurança da informação ou estrutura equivalente serão definidos em ato administrativo próprio emitido pela organização.

Art. 23. Compete às unidades da organização, no âmbito de suas competências regimentais:

I - atuar para assegurar a conformidade contínua com esta Política e com as normas, procedimentos e orientações internas de segurança da informação;

II - participar dos processos institucionais de gestão de ativos de informação, gestão de riscos, gestão de incidentes e demais instrumentos de gestão de segurança da informação; e

III - adotar, na concepção, implantação e operação de sistemas, processos e serviços, as medidas técnicas e organizacionais necessárias à segurança da informação, observadas as diretrizes desta Política e das normas dela decorrentes.

[listar outras atribuições que julgar necessário]

Parágrafo único. As unidades da organização devem ser capazes de demonstrar, a qualquer tempo, a adoção de medidas eficazes de segurança da informação, mediante registros formais, evidências documentais e relatórios internos.

Art. 24. Compete aos gestores de unidades da organização:

I - implementar o PGSI e respectivas medidas de segurança da informação no âmbito de sua unidade, em conformidade com esta Política e com as normas dela decorrentes;

II - promover o cumprimento, no âmbito de sua unidade, das responsabilidades previstas nos termos do art. 23 desta Política;

III - colaborar com o Gestor de Segurança da Informação no atendimento a demandas de auditoria e de órgãos de controle;

IV - assegurar que os colaboradores sob sua gestão participem das ações de capacitação e de conscientização em segurança da informação adequadas aos seus papéis e responsabilidades; e

V - comunicar tempestivamente à ETIR fatos que possam comprometer a segurança da informação no âmbito de sua unidade.

Art. 25. Compete a todo aquele que utiliza os ativos de informação geridos pela organização conhecer, cumprir e fazer cumprir esta Política, bem como as normas específicas de segurança da informação da organização.

Art. 26. Aquele que, de qualquer forma, tiver ciência sobre incidentes de segurança da informação deverá comunicá-lo à ETIR, seguindo as orientações expedidas pelo [comitê de segurança da informação ou estrutura equivalente] em norma específica.

[listar outros papéis e responsabilidades que julgar necessário]

CAPÍTULO VIII

DISPOSIÇÕES FINAIS

Art. 27. Esta Política e suas atualizações, bem como normas internas específicas de segurança da informação, devem ser amplamente divulgadas ao seu público-alvo.

Art. 28. Esta Política deve ser revisada e atualizada periodicamente a cada [3 (três)] anos ou quando eventos ou mudanças significativas assim o exigirem.

Art. 29. O descumprimento das disposições desta Política, bem como das normas decorrentes, sujeitará o infrator às sanções administrativas, disciplinares, contratuais ou legais cabíveis, na forma da legislação vigente.

Art. 30. Quaisquer exceções a esta Política deverão 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. 31. 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