Modelo de Programa de Governança em 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, 30 de junho de 2026

MODELO DE PROGRAMA DE GOVERNANÇA EM 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
Anderson Souza de Araújo
Ricardo Borges Almeida

EQUIPE DE REVISÃO
Marta Juvina de Medeiros

Histórico de versões

Data	Versão	Descrição	Autor
30/06/2026	1.0	Elaboração do Modelo de Programa de Governança em Segurança da Informação.	Equipe Técnica de Elaboração

Licença *Creative Commons*

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

Medidas do *framework* do PPSI 2.0 apoiadas por esse documento

Controle	Id	Medida	Segmento
0	0.9	O órgão possui Programa de Governança em Segurança da Informação (PGSI)?	Base

Orientações

Esta seção consigna informações básicas para a elaboração do Programa de Governança em Segurança da Informação (PGSI) 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 0.9 do *framework* do PPSI 2.0;
3. recomenda-se que o PGSI seja aprovado por instância colegiada de governança em segurança da informação, ou estrutura equivalente, assegurando legitimidade, alinhamento institucional e respaldo da alta administração ao Programa;
4. as informações sobre diagnósticos de maturidade, planos de trabalho e indicadores do PPSI encontram-se classificadas no grau de sigilo do tipo reservado, nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação, LAI), de seu regulamento e dos normativos aplicáveis – conforme Termos de Classificação de Informação disponíveis no Painel Róis de Informações Classificadas e Desclassificadas do Poder Executivo Federal[2]. Nesse contexto, a utilização deste modelo pelo órgão ou entidade para elaborar, tramitar, armazenar e divulgar o PGSI deve observar os critérios de controle de acesso e proteção aplicáveis às informações classificadas no âmbito da Administração Pública Federal, em especial aos procedimentos dispostos no **Decreto nº 7.845, de 14 de novembro de 2012**;
5. 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 do programa, a capa, esta página e a página final.

[2] https://governa.presidencia.gov.br/painel_publico/#/98b55d08-0983-4287-8f0d-dbdbdabb76d3/53192575-47d7-48ec-b8e9-b0a04c4ee1e2

Programa de Governança em Segurança da Informação do [órgão ou entidade]

Período de vigência: [aaaa]–[aaaa]

Sumário

[Instrução: para atualizar o sumário no Microsoft Word, posicionar o cursor sobre o sumário e pressionar a tecla F9, ou clicar com o botão direito e selecionar “Atualizar campo”.]

1 Introdução

A segurança da informação constitui elemento essencial para a continuidade dos serviços públicos, para a proteção das informações sob custódia do Estado e para a preservação da confiança da sociedade. No âmbito da Administração Pública Federal, esse tema, de natureza transversal, demanda integração à estratégia organizacional e ao processo institucional de gestão de riscos, articulando objetivos institucionais, requisitos legais e práticas operacionais.

Em resposta a esse desafio, o Programa de Privacidade e Segurança da Informação (PPSI 2.0), instituído pela Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025, estabelece o *framework* de referência para os órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), organizado em três segmentos:

- o segmento base, com medidas estruturantes de governança aplicáveis tanto à privacidade e proteção de dados pessoais quanto à segurança da informação;
- o segmento de segurança da informação, composto por dezoito controles e respectivas medidas distribuídas em três grupos de implementação (GI 1, GI 2 e GI 3); e
- o segmento de privacidade, composto por sete controles e respectivas medidas, voltado à conformidade do tratamento de dados pessoais com a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), e com as resoluções da Agência Nacional de Proteção de Dados (ANPD).

O presente Programa de Governança em Segurança da Informação (PGSI) do [órgão ou entidade] – em conformidade com o disposto no art. 45 da Instrução Normativa GSI/PR nº 3, de 28 de maio de 2026 –, tem por finalidade traduzir os resultados do diagnóstico de maturidade de segurança da informação em ações estruturadas, priorizadas e monitoráveis, definindo responsáveis, prazos, recursos e indicadores associados à implementação das medidas do *framework* do PPSI 2.0. Configura-se, assim, como instrumento de governança integrado à estratégia organizacional e aos processos institucionais de gestão de riscos, que articula diagnóstico, planejamento e monitoramento da segurança da informação no âmbito institucional e assegura alinhamento entre objetivos estratégicos, requisitos legais e práticas operacionais.

O PGSI tem como foco as medidas do segmento de segurança da informação e as medidas do segmento base de natureza correlata, disciplinadas pela Instrução Normativa SGD/MGI nº 4, de 14 de janeiro de 2026, abrangendo tanto as medidas priorizadas para implementação no ciclo vigente quanto aquelas em regime de gestão contínua, voltadas à manutenção da efetividade das medidas e à sustentação dos níveis de implementação alcançados ou almejados.

Destaca-se que o presente Programa observa a articulação entre dois marcos temporais distintos. O primeiro é o ciclo anual de implementação do *framework* do PPSI 2.0, disciplinado por instrução normativa específica editada anualmente pela Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), que prioriza as medidas a serem implementadas no respectivo período no âmbito dos órgãos e entidades do SISP. O segundo é o período de vigência do presente PGSI, fixado em [N] anos, compreendendo o intervalo de [aaaa] a [aaaa], durante o qual incidem múltiplos ciclos anuais e que constitui o

horizonte institucional adotado pela organização para o planejamento, a execução e o monitoramento das medidas de segurança da informação.

Ressalta-se, ainda, que as informações sobre diagnósticos de maturidade, planos de trabalho e indicadores do PPSI constantes deste Programa – classificadas no grau de sigilo do tipo reservado nos Termos de Classificação da Informação (TCIs) disponíveis no Painel Róis de Informações Classificadas e Desclassificadas do Poder Executivo Federal[3] – deverão ser tratadas em conformidade com o regime de proteção de informações classificadas estabelecido na legislação vigente. Os agentes públicos que tenham acesso às informações classificadas devem adotar as medidas de segurança necessárias à sua proteção, incluindo controles de acesso, armazenamento adequado, restrição de circulação e cuidados na comunicação e no uso de sistemas informacionais. O descumprimento das disposições relativas ao tratamento de informações classificadas sujeitará o agente público às responsabilidades administrativas, civis e penais cabíveis, nos termos da Lei nº 12.527, de 2011, do Decreto nº 7.724, de 2012, e do Decreto nº 7.845, de 2012.

[Instrução: o órgão ou entidade pode complementar esta seção com breve contextualização institucional, indicando, por exemplo, sua missão, principais processos finalísticos, criticidade dos ativos de informação custodiados, ou outros elementos relevantes à introdução e ao escopo do PGSI.]

[3] https://governa.presidencia.gov.br/painel_publico/#/98b55d08-0983-4287-8f0d-dbdbdabb76d3/53192575-47d7-48ec-b8e9-b0a04c4ee1e2

2 Diagnóstico do PPSI

Esta seção apresenta o resultado do diagnóstico de maturidade em segurança da informação realizado pela organização no período de [mês/ano] a [mês/ano], com base no *framework* do PPSI 2.0. O diagnóstico fundamenta a definição das ações do PGSI, permitindo a identificação estruturada das oportunidades de melhoria, e subsidia a priorização das ações no âmbito do Programa.

As informações constantes nesta seção foram extraídas do Sistema do Programa de Privacidade e Segurança da Informação (SisPPSI) e refletem a situação verificada no referido período.

2.1 Síntese da situação atual

O diagnóstico das medidas do segmento de segurança da informação foi conduzido pelo gestor de segurança da informação, conforme competência estabelecida no art. 10 da Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025, [com apoio da unidade responsável pela segurança da informação] e com a participação das unidades [listar unidades técnicas e de negócio envolvidas], abrangendo os dezoito controles de segurança da informação previstos no *framework* do PPSI 2.0.

Além disso, o diagnóstico das medidas do segmento base do *framework* de natureza correlata à segurança da informação foi conduzido pelo responsável setorial pela gestão da integridade, conforme competência estabelecida no art. 12 da Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025, com a participação do gestor de segurança da informação e [com a colaboração da unidade responsável pela segurança da informação] e [das demais unidades envolvidas, conforme aplicável].

A Tabela 1 apresenta o nível de adoção dos controles do segmento de segurança da informação. Optou-se por não consolidar nesta visão as medidas do segmento base, dada a sua natureza híbrida – abrangendo aspectos correlatos tanto à segurança da informação quanto à privacidade –, o que tornaria imprecisa a apresentação por controle. Desta forma, as medidas do segmento base são apresentadas individualmente, no que couber, na subseção 2.3.

Tabela 1: nível atual de adoção dos controles

ID do controle	Título do controle	Nível atual
1	Inventário de ativos institucionais	[0-5]
2	Inventário de soluções de software	[0-5]
3	Proteção de dados	[0-5]
4	Configuração segura de ativos e soluções de software	[0-5]

ID do controle	Título do controle	Nível atual
5	Gestão de contas	[0-5]
6	Gestão de acesso	[0-5]
7	Gestão contínua de vulnerabilidades	[0-5]
8	Gestão de registros de auditoria	[0-5]
9	Proteção de e-mail e navegador web	[0-5]
10	Defesa contra malware	[0-5]
11	Recuperação de dados	[0-5]
12	Gestão de infraestrutura de rede	[0-5]
13	Monitoramento e defesa da rede	[0-5]
14	Conscientização e treinamento de competências	[0-5]
15	Gestão de provedor de serviços	[0-5]
16	Segurança de aplicações	[0-5]
17	Gestão de incidentes	[0-5]
18	Testes de intrusão	[0-5]

2.2 Indicadores e visualizações do diagnóstico

Esta subseção apresenta os elementos visuais e os indicadores quantitativos que subsidiam a análise da implementação das medidas e a comunicação dos resultados às instâncias de governança do PGSI.

[Instrução: recomenda-se incluir nesta subseção:

- gráfico-radar (ou similar) com o nível de adoção dos controles;
- histograma com a distribuição dos níveis de implementação por medida;
- evolução comparativa em relação a ciclos anteriores, quando aplicável;
- painéis de indicadores institucionais relacionados à segurança da informação.]

2.3 Medidas para implementação no período de vigência

Com base no diagnóstico apresentado nas subseções 2.1 e 2.2, e em observância às medidas priorizadas pela Instrução Normativa SGD/MGI nº 4, de 14 de janeiro de 2026, foi definida a organização institucional das medidas para implementação no período de vigência deste PGSI, conforme a Tabela 2, que orientará a elaboração do plano de trabalho detalhado constante da subseção 3.1.

A Tabela 2 apresenta, para cada medida, o nível atual de implementação, verificado no diagnóstico, e o nível-alvo, com vistas ao atingimento do nível aprimorado, nos termos do § 4º do art. 6º da Instrução Normativa SGD/MGI nº 4, de 14 de janeiro de 2026 – observadas a realidade institucional da organização e o plano de trabalho submetido no SisPPSI. Apresenta-se, ainda, a coluna de justificativa institucional destinada ao registro das justificativas de priorização institucional e, excepcionalmente, da justificativa para a indicação de nível-alvo inferior ao aprimorado.

[Instrução: a Tabela 2, a seguir, apresenta três exemplos de medidas, com base nas medidas 1.1, 1.3 e 6.3 do *framework* do PPSI 2.0, exclusivamente para fins demonstrativos. O órgão ou entidade deve substituir integralmente os exemplos pelos registros correspondentes às medidas identificadas para implementação no período de vigência do PGSI, mantendo a coerência com o diagnóstico submetido no SisPPSI.]

Tabela 2: medidas para implementação no período de vigência do PGSI

Medida	Nível atual	Nível-alvo	Justificativa institucional
[1.1 O órgão estabelece e mantém um inventário detalhado de ativos institucionais?]	[2]	[5]	[Medida fundacional do framework (GI 1); inventário existente é parcial e não inclui todos os ativos críticos.]
[1.3 O órgão usa ferramenta de descoberta ativa para identificação de ativos institucionais?]	[1]	[5]	[Medida correlata atendida pela mesma ação que implementa a medida 1.1, conforme ficha 3.1.1.]
[6.3 O órgão exige autenticação multifator (*Multi-Factor Authentication,* MFA) para soluções de software expostas externamente?]	[1]	[5]	[Medida GI 1 com elevado impacto na redução de risco de comprometimento de credenciais; exigência regulatória correlata.]
[ ]	[ ]	[ ]	[ ]
[ ]	[ ]	[ ]	[ ]

O diagnóstico apresentado nesta seção consolida a visão institucional sobre a maturidade em segurança da informação, evidencia as oportunidades de melhoria identificadas a partir da Tabela 2 e estabelece a base para a definição das ações que serão detalhadas na seção 3.

3 Planejamento

Como ressaltado previamente, o PGSI é instrumento de governança que orienta a implementação e o acompanhamento das ações de segurança da informação de forma alinhada ao planejamento estratégico institucional, aos objetivos organizacionais, ao processo de gestão de riscos corporativos e às diretrizes de governança pública, assegurando que a segurança da informação seja tratada de forma integrada, transversal e coerente com a missão institucional.

O planejamento do PGSI tem por finalidade transformar as lacunas identificadas no diagnóstico em ações estruturadas, com responsáveis, prazos, recursos, indicadores e mecanismos de monitoramento claramente definidos.

Cada ação planejada está explicitamente vinculada a uma ou mais medidas do *framework* do PPSI 2.0, assegurando rastreabilidade entre diagnóstico, planejamento e execução. As ações observam, de forma integrada, o nível de risco associado às medidas identificadas, a criticidade dos ativos envolvidos, a dependência entre ações e medidas, as exigências legais e normativas, a capacidade operacional e orçamentária do órgão e as medidas do ciclo de implementação definido pela Instrução Normativa SGD/MGI nº 4, de 14 de janeiro de 2026.

3.1 Plano de trabalho detalhado

Nesta subseção são apresentados, para todas as medidas identificadas na Tabela 2 da subseção 2.3, os registros detalhados dos planos de trabalho das ações deste PGSI, contemplando a vinculação ao diagnóstico, o objetivo da ação, a descrição das atividades, as responsabilidades, os recursos necessários, os prazos, os indicadores de acompanhamento e a situação da execução.

[Instrução: a seguir são apresentados dois exemplos de fichas de plano de trabalho – contendo dados hipotéticos, opções ou orientações de preenchimento –, com base nas medidas 1.1, 1.3 e 6.3 do framework do PPSI 2.0, exclusivamente para fins demonstrativos. O órgão ou entidade deve replicar a estrutura para cada ação planejada para o período de vigência do PGSI, substituindo integralmente o conteúdo dos campos pelo registro correspondente ao caso concreto. Note que uma ação pode atender a mais de uma medida prevista no diagnóstico.]

3.1.1 Ação [1] – Ficha de plano de trabalho

Título da ação	[Estabelecer inventário centralizado e auditável de ativos institucionais]
Medidas atendidas	[1.1, 1.3]
Descrição da situação atual	[Há inventário parcial, mantido em planilha eletrônica, sem rotina formal de atualização e sem cobertura de ambientes em nuvem.]
Descrição da ação	[1) Definir o escopo de ativos a serem inventariados (servidores, estações, dispositivos de rede, ativos em nuvem IaaS/PaaS); 2) selecionar e implantar ferramenta de descoberta automatizada compatível com o

	ambiente; 3) elaborar e publicar processo formal de gestão do inventário; 4) realizar primeira carga consolidada do inventário; 5) instituir rotina semestral de revisão e validação.]
Responsável principal	[unidade responsável pela infraestrutura de TI]
Unidades envolvidas	[unidade responsável pela segurança da informação; unidade responsável pelo patrimônio]
Recursos humanos	[quantitativo e perfil estimados]
Recursos tecnológicos	[ferramenta X de descoberta automatizada de ativos; integração com CMDB, quando aplicável]
Recursos orçamentários	[valor estimado, fonte e dotação]
Necessidade de contratação	[Sim / Não - justificar]
Data de início	[dd/mm/aaaa]
Data de conclusão prevista	[dd/mm/aaaa]
Indicador de acompanhamento	[Percentual de ativos institucionais cobertos pelo inventário centralizado, com meta de 95% na data de conclusão, verificado por relatório trimestral extraído da ferramenta.]
Situação da execução	[Não iniciada / Em execução / Concluída / Suspensa]
Limitações e riscos residuais	[Ativos transitórios em ambientes de teste podem permanecer fora do inventário automatizado, demandando registro manual e revisões periódicas. Risco residual a ser formalmente aceito pelo Comitê de Segurança da Informação ou estrutura equivalente.]
Observações	[Possibilidade de correlação com a medida “2.1 - Inventário de soluções de software”. A adoção da ferramenta de descoberta automatizada pode permitir o atendimento simultâneo da medida 2.1.]

3.1.2 Ação [2] – Ficha de plano de trabalho

Título da ação	[Implantar MFA em soluções expostas externamente]
Medidas atendidas	[6.3]

Descrição da situação atual	[Existe decisão formal de adoção, mas a implementação ainda não foi iniciada nos sistemas expostos externamente.]
Descrição da ação	[1) Inventariar as soluções expostas externamente; 2) avaliar capacidade de integração com o provedor de identidade institucional ou serviço de SSO; 3) definir mecanismo de MFA padrão (TOTP, push, FIDO2); 4) implantar progressivamente, iniciando por sistemas críticos; 5) comunicar e capacitar usuários; 6) monitorar adesão e tratar exceções.]
Responsável principal	[unidade responsável pela infraestrutura de TI]
Unidades envolvidas	[unidade responsável pela segurança da informação; unidade responsável pelos sistemas de informação; unidade de comunicação]
Recursos humanos	[quantitativo e perfil estimados]
Recursos tecnológicos	[provedor de identidade institucional; tokens FIDO2 ou solução TOTP; integração com SSO]
Recursos orçamentários	[valor estimado, fonte e dotação]
Necessidade de contratação	[Sim / Não - justificar]
Data de início	[dd/mm/aaaa]
Data de conclusão prevista	[dd/mm/aaaa]
Indicador de acompanhamento	[Percentual de soluções expostas externamente com MFA habilitado, com meta de 100% na data de conclusão, verificado por relatório mensal do provedor de identidade.]
Situação da execução	[Não iniciada / Em execução / Concluída / Suspensa]
Limitações e riscos residuais	[Risco residual: usuários sem dispositivo móvel exigirão mecanismo alternativo de autenticação, com controles compensatórios previstos.]
Observações	[Correlação com as medidas “5.6 - Centralização da gestão de contas” e “6.7 - Centralização do controle de acesso”.]

3.1.3 Ação [X] – Ficha de plano de trabalho

[Instrução: replicar a estrutura das fichas 3.1.1 e 3.1.2 para cada uma das demais ações que serão realizadas para implementação das medidas apresentadas na subseção 2.3.

Recomenda-se manter a numeração sequencial das subseções (3.1.3, 3.1.4, e assim sucessivamente).]

3.2 Cronograma consolidado

A Tabela 3 apresenta a consolidação das ações previstas nas fichas de plano de trabalho da subseção 3.1, em conjunto com as respectivas datas de início, de conclusão e responsável, objetivando uma visão integrada da execução do plano e a identificação de eventuais sobreposições e dependências críticas.

Tabela 3: síntese das ações planejadas

ID da ação	Título da ação	Início	Conclusão	Responsável
[1]	[Estabelecer inventário centralizado e auditável de ativos institucionais]	[mm/aaaa]	[mm/aaaa]	[unidade]
[2]	[Implantar MFA em soluções expostas externamente]	[mm/aaaa]	[mm/aaaa]	[unidade]
[ ]	[ ]	[ ]	[ ]	[ ]

4 Monitoramento e melhoria contínua

O monitoramento e a melhoria contínua do PGSI têm por objetivo assegurar a execução, a avaliação e o aprimoramento sistemático das ações planejadas, garantindo que o Programa não se limite à implementação inicial de medidas – mas se mantenha atual, efetivo e aderente à evolução do ambiente institucional, tecnológico e regulatório. O acompanhamento deve ser realizado de forma estruturada, com base em relatórios de execução, evidências documentais ou resultados de auditorias.

Destaca-se que a efetividade do PGSI depende do comprometimento da alta administração, da atuação coordenada das unidades organizacionais envolvidas e do engajamento dos agentes públicos em sua implementação e manutenção. O acompanhamento da execução do plano de trabalho deve ser realizado por meio dos indicadores definidos em cada ficha de plano de trabalho, consolidados em relatório periódico submetido ao [Comitê de Segurança da Informação ou estrutura equivalente].

As revisões do PGSI ocorrem em três modalidades:

- a primeira modalidade é a revisão anual ordinária, realizada após a publicação de instrução normativa específica de novo ciclo de implementação pela SGD/MGI, e tem por finalidade atualizar o diagnóstico, incorporar as medidas priorizadas no novo ciclo, ajustar os planos de trabalho e atualizar o cronograma consolidado, gerando nova versão do PGSI;
- a segunda, por sua vez, é a revisão integral do PGSI, realizada ao final do seu período de vigência ([aaaa]), e consiste na elaboração de novo PGSI para o período subsequente, precedido de novo diagnóstico; e
- a terceira modalidade é a revisão extraordinária, motivada por alterações relevantes no contexto institucional, tecnológico ou regulatório, ou em decorrência de incidentes de alto impacto.

5 Conclusão

O presente PGSI consolida a abordagem institucional do [órgão ou entidade] para a gestão da segurança da informação, em conformidade com o *framework* do PPSI 2.0, articulando diagnóstico de maturidade, plano de trabalho detalhado e mecanismos de monitoramento. Por meio deste documento, a organização reafirma a segurança da informação como tema estratégico, integrado à missão institucional e à gestão pública.

Ao estruturar diretrizes estratégicas, diagnóstico de maturidade, planejamento, monitoramento e mecanismos de melhoria contínua, o PGSI adota um modelo orientado à gestão por resultados, permitindo que os controles e medidas de segurança da informação sejam conduzidos de forma planejada, priorizada e monitorável. Essa abordagem contribui para a proteção dos ativos de informação, a redução de riscos de segurança da informação, o fortalecimento da conformidade legal e normativa e o aumento da maturidade e da resiliência organizacional.

[Instrução: recomenda-se ao órgão ou entidade apresentar nesta seção, em poucos parágrafos, uma síntese com base nos dados concretos do seu diagnóstico e plano de trabalho.]

gov.br

Dúvida?

Entre em contato conosco

Sítio PPSI:

PPSI 2.0 - Governo Digital