DIÁRIO OFICIAL DA UNIÃO

Publicado em: 31/10/2025 | Edição: 208 | Seção: 1 | Página: 91

Órgão: Ministério da Gestão e da Inovação em Serviços Públicos/Secretaria de Governo Digital

PORTARIA SGD/MGI Nº 9.511, DE 28 DE OUTUBRO DE 2025

Institui o Programa de Privacidade e Segurança da Informação no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional, que possuem unidades que integram o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo federal.

O SECRETÁRIO DE GOVERNO DIGITAL DO MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS, no uso das atribuições que lhe conferem o art. 23, caput, inciso VI, do Decreto nº 12.102, de 8 de julho de 2024, o art. 3º, caput, inciso VI, do Decreto 12.198, de 24 de setembro de 2024, e o art. 4º, caput, incisos I, III, IV e V do Decreto nº 7.579, de 11 de outubro de 2011, e tendo em vista o disposto na Portaria GSI/PR nº 93, de 18 de outubro de 2021, resolve:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Portaria institui o Programa de Privacidade e Segurança da Informação - PPSI no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional, que possuem unidades que integram o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo federal.

Art. 2º Para fins desta Portaria, consideram-se:

I - controle de privacidade: conjunto de medidas técnicas e administrativas para a proteção de dados pessoais em ativos de informação;

II - controle de segurança da informação: conjunto de medidas técnicas e administrativas para assegurar a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações;

III - informações críticas sobre privacidade e segurança da informação: quaisquer dados ou informações sobre infraestrutura, configurações e características técnicas dos ativos de informação, políticas, normas e procedimentos operacionais e arquiteturas de negócio que podem expor vulnerabilidades e comprometer a privacidade dos titulares ou a confidencialidade, a integridade, a disponibilidade ou a autenticidade das informações;

IV - medida de privacidade: ação técnica ou administrativa para proteger dados pessoais contra acessos não autorizados, vazamentos, usos indevidos ou qualquer outra forma de tratamento que possa comprometer a privacidade dos titulares;

V - medida de segurança da informação: ação técnica ou administrativa para assegurar a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações; e

VI - plano de trabalho: instrumento tático de planejamento da implementação das medidas de privacidade e de segurança da informação.

CAPÍTULO II

DO PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Art. 3º O PPSI caracteriza-se como um conjunto de ações, iniciativas e estratégias distribuídas nas áreas temáticas de governança, maturidade, metodologia, pessoas e tecnologia.

§ 1º O PPSI tem como objetivo elevar a maturidade e a resiliência dos órgãos e entidades da administração pública federal direta, autárquica e fundacional, que possuem unidades que integram o SISP, nos aspectos de privacidade e segurança da informação.

§ 2º São iniciativas do PPSI:

I - definir e manter a estrutura de controles e medidas de privacidade e segurança da informação, além de metodologias e ferramentas de apoio;

II - diagnosticar o grau de implementação das medidas de privacidade e segurança da informação pelos órgãos e entidades do SISP fundamentado em processo de gestão de riscos;

III - acompanhar a implementação das medidas de privacidade e segurança da informação;

IV - orientar a estrutura de governança do PPSI, prevista no art. 7º, quanto às melhores práticas relacionadas à privacidade e segurança da informação;

V - fomentar a integração da gestão de riscos em privacidade e segurança da informação com a gestão de riscos do órgão ou entidade;

VI - promover parcerias com órgãos e entidades públicas, instituições privadas e organismos internacionais para desenvolver e dar sustentação às iniciativas relacionadas aos temas, nos termos da legislação vigente;

VII - promover a cultura e as boas práticas em privacidade e segurança da informação;

VIII - estabelecer e coordenar o Centro de Excelência em Privacidade e Segurança da Informação do Governo Digital;

IX - estabelecer e coordenar o Centro Integrado de Segurança Cibernética do Governo Digital;

X - apoiar na prevenção, tratamento e resposta a incidentes cibernéticos; e

XI - identificar e disseminar informações sobre ameaças e vulnerabilidades para a prevenção, tratamento e resposta a incidentes cibernéticos.

§ 3º São valores do PPSI:

I - a soberania;

II - a maturidade;

III - a resiliência;

IV - a inteligência;

V - a efetividade; e

VI - a colaboração.

Art. 4º O PPSI constitui instrumento de governança dos órgãos e entidades da administração pública federal direta, autárquica e fundacional, e deve ser implementado em conformidade com políticas, normas e sistemas aplicáveis, incluindo, mas não se limitando:

I - à Lei nº 13.709, de 14 de agosto de 2018;

II - à Lei nº 14.129, de 29 de março de 2021;

III - ao Decreto nº 9.203, de 22 de novembro de 2017;

IV - ao Decreto nº 11.856, de 26 de dezembro de 2023;

V - ao Decreto nº 12.572, de 4 de agosto de 2025;

VI - ao Decreto nº 12.573, de 4 de agosto de 2025; e

VII - aos normativos emitidos pelo Gabinete de Segurança Institucional da Presidência da República relacionados à segurança da informação e pela Agência Nacional de Proteção de Dados.

Art. 5º As informações críticas geradas a partir da execução de quaisquer etapas, atividades ou procedimentos previstos nesta Portaria são consideradas imprescindíveis à segurança da sociedade e do Estado e somente podem ser acessadas por profissionais autorizados pelas autoridades responsáveis pelos respectivos ativos de informação, conforme previsto no art. 15 do Decreto nº 10.748, de 16 de julho de 2021.

Art. 6º A Secretaria de Governo Digital atua no apoio técnico à realização das ações, iniciativas e estratégias do Programa, em articulação com a estrutura de governança do PPSI dos órgãos e entidades.

CAPÍTULO III

ESTRUTURA DE GOVERNANÇA DO PPSI

Art. 7º Compõem a estrutura de governança do PPSI:

I - a alta administração, nos termos do art. 2º, caput, inciso III, do Decreto nº 9.203, de 22 de novembro de 2017;

II - o gestor de tecnologia da informação e comunicação, de que trata o art. 4º, caput, inciso IV, da Portaria SGD/ME nº 778, de 4 de abril de 2019;

III - o gestor de segurança da informação, de que trata a Instrução Normativa nº 1, de 27 de maio de 2020;

IV - o encarregado pelo tratamento de dados pessoais, de que trata o art. 41, § 2º, da Lei nº 13.709, de 14 de agosto de 2018; e

V - o responsável setorial pela gestão da integridade, de que trata o art. 5º, caput, inciso II, do Decreto nº 11.529, de 16 de maio de 2023.

Art. 8º À alta administração compete gerir os riscos no âmbito organizacional, fornecer os recursos necessários para assegurar a gestão da privacidade e da segurança da informação, viabilizar a implementação da estrutura de governança do PPSI e adotar decisões sobre privacidade e segurança da informação em um nível de relevância e prioridade adequadas e alinhadas com a estratégia e com a consecução dos objetivos do órgão ou entidade no cumprimento da sua missão institucional.

Art. 9º Ao gestor de tecnologia da informação e comunicação compete planejar, desenvolver, executar e monitorar as medidas de privacidade e segurança da informação em soluções de tecnologia da informação e comunicação, considerando inclusive a cadeia de suprimentos relacionada à solução.

Art. 10. Ao gestor de segurança da informação compete conduzir o diagnóstico de segurança da informação, bem como orientar, planejar e monitorar as medidas de segurança da informação.

Art. 11. Ao encarregado pelo tratamento de dados pessoais compete conduzir o diagnóstico de privacidade, bem como orientar os agentes de tratamento no planejamento, implementação e monitoramento das medidas de privacidade.

Art. 12. Ao responsável setorial pela gestão da integridade compete o diagnóstico das medidas relativas à estruturação básica e instrumentos fundamentais de governança do PPSI, além da coordenação e gestão dos riscos para a integridade relacionados aos temas.

CAPÍTULO IV

DO FRAMEWORK DO PPSI

Art. 13. O framework do PPSI é composto por um conjunto de controles e medidas de privacidade e segurança da informação.

Art. 14. Os órgãos e entidades da administração pública federal direta, autárquica e fundacional, que possuem unidades que integram o SISP, devem adotar o framework de privacidade e de segurança da informação, sendo sua gestão sob responsabilidade da estrutura de governança do PPSI.

Art. 15. Consideram-se etapas para a execução do framework:

I - diagnóstico: o órgão ou entidade deve executar o diagnóstico, considerando o modelo de avaliação disponibilizado por meio do framework;

II - análise de lacunas: identificar, a partir do diagnóstico previsto no inciso I do caput, a necessidade de implementação de medidas ou de aprimoramento das medidas já implementadas de privacidade e segurança da informação, para aumento da maturidade do órgão ou entidade;

III - planejamento: a partir da etapa prevista no inciso II do caput, planejar e especificar os prazos e os recursos necessários à implementação das medidas, considerando aspectos orçamentários e de recursos humanos do próprio órgão ou entidade; e

IV - implementação: implementar medidas priorizadas e gerenciar as medidas já implementadas, conforme planejamento previsto no inciso III do caput, para aumento da maturidade do órgão ou entidade nos aspectos de privacidade e segurança da informação.

Parágrafo único. A Secretaria de Governo Digital poderá definir o conjunto de medidas prioritárias a serem implementadas pelos órgãos e entidades da administração pública federal direta, autárquica e fundacional que possuem unidades que integram o SISP, bem como outras orientações necessárias para a adequada implementação do PPSI.

Art. 16. O diagnóstico e o plano de trabalho resultante da etapa de planejamento devem ser encaminhados à Secretaria de Governo Digital, conforme definido por esta Secretaria.

§ 1º O plano de trabalho para implementar as medidas do framework deve ser integrado aos instrumentos de planejamento institucional do órgão ou entidade.

§ 2º As ações decorrentes do plano de trabalho que demandem a necessidade de contratação de solução de tecnologia da informação e comunicação devem ser vinculadas ao Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC do órgão ou entidade.

Art. 17. A Secretaria de Governo Digital pode solicitar evidências da implementação das medidas de privacidade e segurança da informação para fins de análise, monitoramento e adequação do apoio ao PPSI.

CAPÍTULO V

DO CENTRO INTEGRADO DE SEGURANÇA CIBERNÉTICA DO GOVERNO DIGITAL

Art. 18. Fica instituído o Centro Integrado de Segurança Cibernética do Governo Digital - CISC gov.br, como uma unidade de coordenação setorial, com o objetivo de integrar e fortalecer as ações de prevenção, tratamento e resposta a incidentes cibernéticos nos órgãos e entidades da administração pública federal direta, autárquica e fundacional que possuem unidades que integram o SISP, nos termos do Decreto nº 10.748, de 16 de julho de 2021.

Parágrafo único. Compete à Secretaria de Governo Digital a prospecção, o planejamento, a implementação, o monitoramento, a melhoria contínua e o gerenciamento das ações no âmbito do CISC gov.br.

Art. 19. Compete ao CISC gov.br:

I - atuar como equipe principal para prevenção, tratamento e resposta a incidentes cibernéticos da Plataforma gov.br e dos demais serviços sob responsabilidade da Secretaria de Governo Digital;

II - apoiar o planejamento, a implementação, a operação, a prevenção, o tratamento e a resposta das equipes de resposta a incidentes cibernéticos dos órgãos e entidades da administração pública federal direta, autárquica e fundacional que possuem unidades que integram o SISP;

III - promover a comunicação e colaboração com outras equipes de prevenção, tratamento e resposta a incidentes cibernéticos, tanto dos órgãos e entidades da administração pública federal direta, autárquica e fundacional quanto das organizações privadas;

IV - estabelecer padrões, procedimentos e processos técnicos, observando os normativos do Gabinete de Segurança Institucional;

V - executar testes de intrusão em ativos de informação, sob demanda;

VI - executar testes estáticos e dinâmicos de segurança em aplicações;

VII - realizar análises não invasiva e contínua de ameaças e vulnerabilidades em ativos de informação;

VIII - realizar análises de ameaças e vulnerabilidades em ativos de informação, sob demanda;

IX - desenvolver atividades de inteligência de ameaças cibernéticas;

X - elaborar e publicar alertas e recomendações;

XI - emitir determinações e prazos para correção de vulnerabilidades com alta criticidade; e

XII - realizar o monitoramento de padrões maliciosos no tráfego externo de rede.

§ 1º Os dispostos no caput não excluem ou substituem as atribuições do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov e das equipes de coordenação setorial previstas no Decreto nº 10.748, de 16 de julho de 2021.

§ 2º O serviço disposto no inciso V do caput só poderá ser realizado sob autorização expressa de autoridade máxima competente pela custódia dos ativos de informação no órgão ou entidade da administração pública federal direta, autárquica e fundacional.

§ 3º Fica autorizada a execução do serviço previsto no inciso VII do caput em todos os órgãos e entidades da administração pública federal direta, autárquica e fundacional que possuem unidades que integram o SISP.

§ 4º O disposto no inciso XII do caput só poderá ser realizado sob autorização expressa de autoridade máxima competente pela custódia dos ativos de informação no órgão ou entidade da administração pública federal direta, autárquica e fundacional, exceto em caso de uso dos serviços de conectividade da infraestrutura de rede óptica de comunicações - Infovia.

Art. 20. Os órgãos e as entidades integrantes do SISP devem notificar ao CISC Gov.br os incidentes cibernéticos identificados.

CAPÍTULO VI

DO CENTRO DE EXCELÊNCIA EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DO GOVERNO DIGITAL

Art. 21. Fica instituído o Centro de Excelência em Privacidade e Segurança da Informação do Governo Digital - CEPS gov.br, com o objetivo de promover a cultura de privacidade e segurança da informação nos órgãos e entidades da administração pública federal direta, autárquica e fundacional que possuem unidades que integram o SISP.

§ 1º As ações do CEPS gov.br devem observar as diretrizes estabelecidas no Decreto nº 9.991, de 28 de agosto de 2019, assim como os demais normativos e legislações vigentes sobre a matéria.

§ 2º Compete à Secretaria de Governo Digital a prospecção, o planejamento, a implementação, o monitoramento, a melhoria contínua e o gerenciamento das ações no âmbito do CEPS gov.br.

Art. 22. Compete ao CEPS gov.br:

I - promover parcerias com órgãos e entidades públicas, instituições privadas e organismos internacionais, nos termos da legislação;

II - fomentar e viabilizar ações de sensibilização, conscientização, capacitação e especialização dos recursos humanos dos órgãos e entidades da administração pública federal direta, autárquica e fundacional que possuem unidades que integram o SISP, em temas relacionados à privacidade e à segurança da informação, considerando o engajamento dos profissionais;

III - fomentar ações de engajamento e capacitação em todos os níveis da estrutura organizacional dos órgãos e entidades, promovendo a mudança cultural voltada à proteção de dados pessoais, ao uso ético, responsável e seguro dos recursos de tecnologia da informação, bem como à execução segura dos processos de trabalho;

IV - apoiar os órgãos e entidades da administração pública federal direta, autárquica e fundacional que possuem unidades que integram o SISP na implementação da estrutura de controles de privacidade e segurança da informação, por meio de ações conjuntas e colaborativas;

V - disseminar conhecimentos sobre boas práticas em privacidade e segurança da informação;

VI - proporcionar jornadas de capacitação em privacidade e segurança da informação para agentes públicos vinculados aos órgãos e entidades da administração pública federal direta, autárquica e fundacional que possuem unidades que integram o SISP;

VII - promover a criação de fóruns especializados em busca de prospectar oportunidades e trocas de experiências e informações; e

VIII - desenvolver exercícios conjuntos de simulações cibernéticas nos órgãos e entidades da administração pública federal direta, autárquica e fundacional que possuem unidades que integram o SISP.

CAPÍTULO VII

DISPOSIÇÕES FINAIS

Art. 23. A implementação e o aprimoramento das medidas de privacidade e segurança da informação são de responsabilidade das unidades organizacionais dos órgãos e entidades da administração pública federal direta, autárquica e fundacional, no escopo de suas competências legais e regimentais.

Art. 24. Os casos omissos serão resolvidos pela Secretaria de Governo Digital.

Art. 25. Fica revogada a Portaria SGD/MGI nº 852, de 28 de março de 2023.

Art. 26. Esta Portaria entra em vigor em 1º de janeiro de 2026.

ROGÉRIO SOUZA MASCARENHAS