DIÁRIO OFICIAL DA UNIÃO

Publicado em: 30/03/2023 | Edição: 62 | Seção: 1 | Página: 92

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

PORTARIA SGD/MGI Nº 852, DE 28 DE MARÇO DE 2023

Dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI

O SECRETÁRIO DE GOVERNO DIGITAL DO MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS, no uso das atribuições que lhe conferem o art. 22 do Decreto nº 11.437, de 17 de março de 2023, e o inciso V do art. 6º do Decreto 10.332, de 28 de abril de 2020, e tendo em vista o disposto no art. 4º do Decreto nº 7.579, de 11 de outubro de 2011, resolve:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Estabelecer o Programa de Privacidade e Segurança da Informação (PPSI), no âmbito dos órgãos e entidades da administração pública federal direta, autárquica e fundacional, que possuem unidades que compõem o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, conforme art. 3º do Decreto nº 7.579, de 11 de outubro de 2011.

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

I - ativos de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

II - controle de privacidade: conjunto de medidas que visam implementar práticas técnicas e gerenciais para a proteção de dados pessoais em ativos de informação;

III - controle de segurança da informação: conjunto de medidas que visam implementar práticas técnicas e gerenciais para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

IV - governo digital: prestação digital de serviços públicos por meio de tecnologias de amplo acesso pela população, nos termos da Lei nº 14.129, de 29 de março de 2021;

V - plano de trabalho: instrumento tático de diagnóstico e planejamento da implementação dos controles de privacidade e de segurança da informação;

VI - plano de transformação digital: instrumento de planejamento alinhado com a Estratégia de Governo Digital, instituída pelo Decreto nº 10.332, de 28 de abril de 2020;

VII - plano diretor de tecnologia da informação e comunicação: instrumento de diagnóstico, planejamento e gestão dos recursos e processos de TIC - Tecnologia da Informação e Comunicação , com o objetivo de atender às necessidades finalísticas e de informação de um órgão ou entidade para um determinado período;

VIII - proteção de dados pessoais, nos termos do inciso LXXIX do art. 5º da Constituição da República Federativa do Brasil de 1988: ações que visam proteger direitos e liberdades fundamentais das pessoas naturais, entre eles a sua privacidade, inclusive em meios digitais;

IX - privacidade: direito à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, nos termos do inciso X do art. 5º da Constituição da República Federativa do Brasil de 1988;

X - segurança cibernética: também conhecido por cibersegurança, são ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a

confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis;

XI - segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XII - soluções de tecnologia da informação e comunicação: conjunto de bens e/ou serviços que apoiam processos de negócio mediante a conjugação de recursos de TIC, nos termos da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, e suas alterações.

Parágrafo único. Os demais termos relacionados à segurança da informação são definidos por meio do Glossário de Segurança da Informação, conforme a Portaria Nº 93 GSI/PR, de 18 de outubro de 2021, e suas alterações.

CAPÍTULO II

DO PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Art. 3º O PPSI tem como objetivo elevar a maturidade e a resiliência dos órgãos e entidades, em termos de privacidade e segurança da informação, no âmbito do SISP.

Art. 4º O PPSI caracteriza-se como um conjunto de projetos e processos distribuídos nas áreas temáticas de governança, maturidade, metodologia, pessoas e tecnologia.

§1º São iniciativas do PPSI:

I - definir e manter a estrutura de controles de privacidade e segurança da informação;

II - estabelecer e coordenar o Centro Integrado de Segurança Cibernética do Governo Digital - CISC Gov.br;

III - diagnosticar o grau de implementação dos controles de privacidade e segurança da informação pelos órgãos e entidades pertencentes ao SISP;

IV - acompanhar a implementação de controles e sensibilizar de forma contínua a Estrutura de Governança, prevista no art. 6º desta Portaria;

V - promover parcerias com órgãos e entidades públicas, entidades privadas e organismos internacionais para desenvolver e dar sustentação às iniciativas relacionadas ao tema, nos termos da legislação;

VI - promover as boas práticas por meio de disponibilização de guias, processos, modelos e procedimentos;

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

VIII - promover a cultura de privacidade e segurança da informação;

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

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

§2º São valores do PPSI:

I - a maturidade;

II - a resiliência;

III - a efetividade;

IV - a colaboração; e

V - a inteligência.

Art. 5º No âmbito da Secretaria de Governo Digital, a Diretoria de Privacidade e Segurança da Informação é a unidade responsável pelo PPSI.

CAPÍTULO III

ESTRUTURA DE GOVERNANÇA DO PPSI

Art. 6º Compõem a Estrutura de Governança do PPSI em cada órgão e entidade da administração pública federal direta, autárquica e fundacional:

I - o Gestor de Tecnologia da Informação e Comunicação, dentre outras atribuições, nos termos da Portaria nº 778, de 4 de abril de 2019, responsável por planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução;

II - o Gestor de Segurança da Informação, dentre outras atribuições, nos termos da Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional, da Presidência da República - GSI/PR, responsável por planejar, implementar e melhorar continuamente os controles de segurança da informação em ativos de informação;

III - o Encarregado pelo Tratamento de Dados Pessoais, dentre outras atribuições, nos termos do art. 41, §2º, da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), responsável por conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis; e

IV - o Responsável pela Unidade Controle Interno, atuará no apoio, supervisão e monitoramento das atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017.

§1º Os agentes públicos listados nos incisos I e II do caput, juntamente com os proprietários de ativos, gestores do negócio ou de políticas públicas, compõem a primeira linha de defesa quando se tratar de controles de privacidade e segurança da informação.

§2º O Encarregado pelo Tratamento de Dados Pessoais desempenha o papel de apoiar as partes citadas no parágrafo anterior com orientações acerca das diretrizes que envolvam privacidade e proteção de dados pessoais nos termos do art. 41 da LGPD.

§3º A Secretaria de Governo Digital, por meio da Diretoria de Privacidade e Segurança da Informação, atuará no apoio ao diagnóstico, no acompanhamento e na prestação de apoio técnico em relação às ações do PPSI no âmbito dos órgãos e entidades, em articulação com a respectiva Estrutura de Governança, considerando o responsável pela unidade de controle interno como ponto focal para intermédio das ações.

CAPÍTULO IV

DO FRAMEWORK DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Art. 7º Institui-se o Framework de Privacidade e Segurança da Informação, composto por um conjunto de controles, metodologias e ferramentas de apoio.

§1º Os controles dispostos no framework deverão ser considerados controles internos da gestão, nos termos do inciso V do art. 2º da Instrução Normativa Conjunta CGU/MPOG nº 1, de 10 de maio de 2016.

§2º Os artefatos e ferramentas que compõem o framework ficarão disponíveis no portal institucional da Secretaria de Governo Digital.

§3º A Secretaria de Governo Digital poderá editar revisões dos artefatos e ferramentas que compõem o framework, com vigência imediata após a publicação e comunicação para os órgãos e as entidades pertencentes ao SISP.

§4º Os controles dispostos no framework deverão observar:

I - a Lei Geral de Proteção de Dados Pessoais;

II - a Política Nacional de Segurança da Informação;

III - os normativos emitidos pela Autoridade Nacional de Proteção de Dados Pessoais e pelo Gabinete de Segurança Institucional; e

IV - as recomendações efetuadas pelos órgãos federais de controle interno e externo.

Art. 8º Os órgãos e as entidades deverão adotar o framework de privacidade de segurança da informação, sendo de responsabilidade da Estrutura de Governança de cada órgão e entidade, nos termos do art. 6º desta Portaria.

Parágrafo único. A decisão de não implementação de medidas consideradas obrigatórias pelo framework deverá ser precedida de adequada motivação com base em análise de riscos.

Art. 9º Considera-se como etapas para a implementação do framework pelos órgãos e entidades pertencentes ao SISP:

I - autoavaliação: execução de avaliação pelo próprio órgão, considerando o modelo de avaliação de maturidade e capacidade disponibilizado por meio do framework;

II - análise de lacunas: a partir da autoavaliação, esta etapa consiste na identificação de oportunidades quanto à necessidade de implementação de medidas ou de melhoria contínua das medidas já implementadas para aumento da capacidade e maturidade do órgão ou entidade;

III - planejamento: após identificadas as oportunidades de melhorias identificadas na etapa anterior, o órgão deve realizar planejamento que especifique o prazo e as necessidades de recursos para implementação, considerando aspectos orçamentários e de recursos humanos do próprio órgão ou entidade; e

IV - implementação: esta etapa consiste na implementação das medidas ou na melhoria contínua de medidas já implementadas para aumento da capacidade e maturidade do órgão.

§1º O órgão ou entidade deverá observar os controles considerados como prioritários pela Secretaria de Governo Digital, em comunicação periódica realizada por meio de ato administrativo para a Estrutura de Governança.

§2º As etapas previstas nos incisos I, II e III do caput deverão ser executadas no prazo de 180 dias a contar da vigência desta Portaria , com possibilidade de prorrogação por igual período, desde que devidamente justificado.

Art. 10. A etapa de planejamento, conforme inciso III do art. 9º, resultará em um plano de trabalho, o qual deverá ser encaminhado à Secretaria de Governo Digital, e revisado continuamente conforme o avanço da implementação e realização de novas autoavaliações.

§1º O plano de trabalho de implementação do framework deverá ser integrado ao Plano de Transformação Digital, ou instrumento equivalente.

§2º As ações decorrentes do plano de trabalho, e que demandem a necessidade de contratação de solução de TIC, serão vinculadas ao Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC.

§3º As Estruturas de Governança do PPSI nos órgãos e entidades deverão prover informações das autoavaliações e do planejamento de modo a subsidiar o acompanhamento realizado pela Secretaria de Governo Digital.

§4º Recomenda-se a avaliação da classificação das informações constantes no plano de trabalho quanto ao grau de sigilo, nos termos dos incisos XI e XII do art.3º do Decreto nº 9.637, de 26 de dezembro de 2018.

§5º O plano de trabalho deverá ser revisado a cada 12 meses, por meio da execução das etapas I, II e III descritas pelo caput do art. 9º.

Art. 11. A Secretaria de Governo Digital promoverá diagnósticos periódicos, em que o órgão deverá executar a etapa de autoavaliação, e acompanhará e apoiará o planejamento e a implementação.

Art. 12. A Secretaria de Governo Digital poderá elaborar e revisar padrões, processos, procedimentos, guias operacionais e ferramentas de apoio para aprimorar o framework de privacidade e segurança da informação.

CAPÍTULO V

DO CENTRO INTEGRADO DE SEGURANÇA CIBERNÉTICA DO GOVERNO DIGITAL

Art. 13. Fica criado no âmbito do PPSI o Centro Integrado de Segurança Cibernética do Governo Digital - CISC Gov.br , caracterizado como uma unidade de coordenação operacional das equipes de prevenção, tratamento e resposta a incidentes cibernéticos dos órgãos e das entidades do Sistema de Administração de Recursos de Tecnologia da Informação - SISP, nos termos da Rede Federal de Gestão de Incidentes Cibernéticos - ReGIC, instituída pelo Decreto nº 10.748, de 16 de julho de 2021.

§1º O CISC Gov.br atuará como equipe principal, nos termos do inciso III do art. 4º da ReGIC, para os serviços que compõem a Plataforma Gov.br e para outros serviços que estejam sob a reponsabilidade da Secretaria de Governo Digital.

§2º Compete à Diretoria de Privacidade e Segurança da Informação da 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. 14. A missão do CISC Gov.br é promover a coordenação das ações de prevenção, tratamento e resposta a incidentes cibernéticos no âmbito do SISP.

Art. 15. As equipes de prevenção, tratamento e resposta a incidentes cibernéticos dos órgãos e das entidades pertencentes ao SISP deverão se integrar às tecnologias, padrões, procedimentos e processos estabelecidos pelo CISC Gov.br, observando os normativos do Gabinete de Segurança Institucional da Presidência da República.

Art. 16. São serviços que compõem o CISC Gov.br:

I - apoio no planejamento, implementação e operação de equipes de prevenção, tratamento e resposta a incidentes cibernéticos nos órgãos e entidades;

II - apoio na prevenção, tratamento e resposta a incidentes cibernéticos;

III - comunicação e colaboração com outras equipes de prevenção, tratamento e resposta a incidentes cibernéticos, tanto dos órgãos e entidades públicas quanto das organizações privadas;

IV - execução de testes de intrusão em ativos de informação, sob demanda;

V - análise não-invasiva e contínua de vulnerabilidades em ativos de informação;

VI - análise de vulnerabilidades em ativos de informação, sob demanda;

VII - atividades de inteligência de ameaças cibernéticas;

VIII - testes estáticos e dinâmicos de segurança em aplicações;

IX - elaboração e publicação de alertas e recomendações; e

X - monitoramento de padrões maliciosos no tráfego externo de rede.

§1º Os serviços dispostos no caput não excluem ou substituem as atribuições do CTIR Gov e das equipes de coordenação setorial previstas pela ReGIC.

§2º O serviço disposto no inciso IV do caput só poderá ser realizado sob autorização expressa de autoridade máxima competente pela custódia dos ativos de informação no órgão ou entidade.

§3º Fica autorizada a execução do serviço previsto no inciso V do caput em todos os órgãos e entidades pertencentes ao SISP.

§4º O serviço disposto no inciso X do caput só poderá ser realizado sob autorização expressa de autoridade máxima competente pela custódia dos ativos de informação no órgão ou entidade, exceto em caso de uso dos serviços de conectividade da Infovia.

Art. 17. O CISC Gov.br poderá emitir determinações e prazos para correção de vulnerabilidades com alta criticidade.

Art. 18. Os órgãos e entidades pertencentes ao SISP deverão notificar ao CISC Gov.br os incidentes cibernéticos identificados.

CAPÍTULO VI

DO CENTRO DE EXCELÊNCIA EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Art. 19. Fica instituído no âmbito do PPSI o Centro de Excelência em Privacidade e Segurança da Informação do Governo Digital, que tem como missão promover a cultura de privacidade e segurança da informação nos órgãos e entidades.

§1º Compete à Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital a prospecção, o planejamento, a implementação, o monitoramento, a melhoria contínua, e o gerenciamento das ações no âmbito do Centro de Excelência.

§2º As ações do Centro de Excelência deverão observar as diretrizes previstas Decreto nº 9.991, de 28 de agosto de 2019 e suas alterações, que dispõe sobre a Política Nacional de Desenvolvimento de Pessoas da administração pública federal direta, autárquica e fundacional, e regulamenta dispositivos da Lei nº 8.112, de 11 de dezembro de 1990, quanto a licenças e afastamentos para ações de desenvolvimento.

Art. 20. São objetivos do Centro de Excelência em Privacidade e Segurança da Informação do Governo Digital:

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

II - fomentar e promover ações de sensibilização, conscientização, capacitação e especialização dos recursos humanos em temas relacionados à privacidade e à segurança da informação, considerando o engajamento e retenção dos profissionais;

III - apoiar os órgãos e entidades para a efetiva implementação da estrutura de controles de privacidade e segurança da informação por meio de ações conjuntas e colaborativas;

IV - fomentar ações de engajamento para promover a mudança cultural em todos os níveis da estrutura organizacional dos órgãos e entidades, para o adequado uso dos recursos de tecnologia e na execução dos processos de trabalho;

V - disseminar conhecimentos sobre as boas práticas nas temáticas de privacidade e segurança da informação;

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

VII - promover exercícios conjuntos de simulações cibernéticas.

CAPÍTULO VII

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 21. Os casos omissos serão resolvidos pela Secretaria de Governo Digital.

Art. 22. Esta Portaria entra em vigor em 3 de abril de 2023.

ROGÉRIO SOUZA MASCARENHAS