DIÁRIO OFICIAL DA UNIÃO

Publicado em: 01/07/2025 | Edição: 121 | Seção: 1 | Página: 104

Órgão: Ministério do Planejamento e Orçamento/Gabinete da Ministra

PORTARIA GM/MPO Nº 181, DE 27 DE JUNHO DE 2025

Institui a Política de Segurança da Informação - POSIN no âmbito do Ministério do Planejamento e Orçamento.

A MINISTRA DE ESTADO DO PLANEJAMENTO E ORÇAMENTO, no uso das atribuições que lhe foram conferidas pelos incisos I e IV do parágrafo único do art. 87 da Constituição Federal, e tendo em vista o disposto na Lei nº 14.600, de 19 de junho de 2023, e no Decreto nº 11.353, de 1º de janeiro de 2023, resolve:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Instituir a Política de Segurança da Informação do Ministério do Planejamento e Orçamento - POSIN, na forma da presente Portaria, a qual tem por finalidade estabelecer princípios, diretrizes, competências e responsabilidades para a gestão da segurança da informação no Ministério.

Art. 2º Esta Política e demais normas associadas aplicam-se a todas as unidades organizacionais do Ministério do Planejamento e Orçamento, devendo ser observada por todos os usuários de informação, incluindo servidores, empregados, colaboradores, prestadores de serviço e quaisquer indivíduos habilitados pelo Ministério para acesso aos ativos de informação sob responsabilidade do órgão.

Art. 3º Para fins desta Política e de suas regulamentações, aplicam-se os termos e definições do Glossário de Segurança da Informação, conforme a Portaria GSI/PR nº 93, de 18 de outubro de 2021.

CAPÍTULO II

dos princípios e diretrizes

Art. 4º As ações de segurança da informação do Ministério devem se orientar pelos princípios constitucionais e administrativos da Administração Pública Federal, bem como pelos seguintes:

I - garantia da disponibilidade, da integridade, da confidencialidade e da autenticidade das informações;

II - eficiência, eficácia, efetividade e economicidade na proteção dos ativos de informação;

III - alinhamento aos objetivos estratégicos e planos institucionais;

IV - resiliência e continuidade dos processos, sistemas, controles de segurança e serviços essenciais;

V - compromisso com a proteção de dados pessoais e privacidade;

VI - observância da publicidade e transparência no trato das informações;

VII - observância do menor privilégio e acesso mínimo necessário a pessoas e sistemas, para o cumprimento de suas funções;

VIII - responsabilidade do usuário da informação pelas práticas que afetam a segurança;

IX - alinhamento às melhores práticas disponíveis;

X - conformidade com estratégias, programas, legislação e normativos vigentes;

XI - observância das competências e especificidades das unidades do Ministério; e

XII - promoção de uma cultura de segurança da informação através de educação e conscientização periódicas.

Art. 5º Os contratos, acordos e instrumentos congêneres firmados pelo Ministério deverão conter cláusulas específicas de conformidade com esta Política, com seus normativos complementares aplicáveis e demais políticas institucionais e legislações de privacidade e proteção de dados pessoais, sempre que cabível.

Parágrafo único. Os atores que compõem a Estrutura de Gestão de Segurança da Informação, definida no artigo 9º, deverão estabelecer os critérios e requisitos das cláusulas de que trata o caput, nos termos da legislação vigente.

Art. 6º A Gestão de Segurança da Informação do Ministério do Planejamento e Orçamento deverá ser constituída, no mínimo, pelos processos relacionados a:

I - gestão de riscos;

II - gestão de ativos;

III - tratamento de informações;

IV - gestão de continuidade;

V - gestão de incidentes de segurança da informação;

VI - gestão da segurança física e do ambiente;

VII - gestão de identidades e acessos;

VIII - gestão do uso dos recursos operacionais, computacionais e de comunicações; e

IX - auditoria e gestão de conformidade.

§ 1º Para cada processo especificado no caput, deve-se observar a elaboração de políticas, planos, normas complementares, procedimentos, manuais e metodologias pertinentes que facilitem seu entendimento e direcionem sua implementação no âmbito do Ministério, conforme competências estipuladas nesta Política.

§ 2 º Os atores que compõem a Estrutura de Gestão de Segurança da Informação, definida no artigo 9º, poderão definir outros processos além daqueles elencados nos incisos do caput, desde que alinhados aos princípios e diretrizes desta Política.

Art. 7º Os processos de gestão de segurança do Ministério devem abordar, no mínimo:

I - a identificação, a quantificação, a priorização, o tratamento, a comunicação e o monitoramento periódico dos riscos;

II - o mapeamento e o inventário de ativos, incluindo o monitoramento das respectivas vulnerabilidades e sua movimentação;

III - a gestão de mudanças nos ativos de informação e nos controles associados, incluindo a garantia de avaliações prévias de segurança;

IV - o tratamento de informações classificadas e de dados pessoais, a privacidade e a transparência e acesso às informações, nos termos da legislação vigente;

V - o estabelecimento de planos de continuidade de negócios e recuperação de desastres, incluindo a realização de testes e exercícios regulares associados aos planos;

VI - a preparação, a identificação, a contenção e a recuperação de incidentes, que deverão compor planos de gestão de incidentes;

VII - o estabelecimento e o gerenciamento de Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR);

VIII - os critérios de comunicação de incidentes às partes interessadas e autoridades competentes;

IX - os perímetros de segurança física e sua proteção;

X - os controles de acesso físico e lógico baseados no menor privilégio;

XI - as políticas de controle de acesso, de uso de senhas e de governança das identidades dos usuários das informações, incluindo segregação de funções e autenticação multifator;

XII - o uso aceitável de e-mail, internet, redes cabeadas e sem fio, acesso remoto, mídias sociais, computação em nuvem, mídias de armazenamento e dispositivos corporativos e pessoais;

XIII - a gestão de segurança de softwares e sistemas de informação adquiridos e desenvolvidos pelo próprio Ministério; e

XIV - a auditoria e conformidade, incluindo planos de verificação e relatórios de avaliação.

Art. 8º As unidades do Ministério que realizam gestão de infraestrutura de rede deverão instituir e manter Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

CAPÍTULO III

DA ESTRUTURA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 9º Fica instituída a Estrutura de Gestão de Segurança da Informação do Ministério do Planejamento - EGSI, composta:

I - pela Alta Administração;

II - pelo Subcomitê de Governança Digital e Segurança da Informação (SGD-SI);

III - pelo Gestor de Segurança da Informação do Ministério (GSIN);

IV - pelas unidades de segurança da informação das secretarias;

V - pelos Gestores de unidades de Tecnologia da Informação e Comunicação, reconhecidos pelo SISP - Sistema de Administração dos Recursos de Tecnologia da Informação;

VI - pelo Encarregado pelo Tratamento de Dados Pessoais;

VII - pelo Responsável pela Unidade de Controle Interno; e

VIII - pelas Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR);

§ 1º O colegiado de que trata o inciso II tem sua definição, composição, funcionamento e competências estabelecidas por meio da Portaria GM/MPO nº 116, de 3 de maio de 2023, alterada pela Portaria GM/MPO nº 162, de 19 de junho de 2023, ou outra que vier a substituí-la.

§ 2 º As unidades de segurança da informação de que trata o inciso IV se referem às unidades organizacionais das secretarias finalísticas e da Secretaria-Executiva do Ministério, existentes ou que vierem a ser constituídas, que tem por missão institucional a atuação na gestão e coordenação da segurança da informação e privacidade de dados, no âmbito de seus órgãos, devendo o Gestor de Segurança da Informação exercer tal papel para aquelas secretarias que não possuem unidade própria de segurança estabelecida.

§ 3 º A participaçaÞo na referida estrutura naÞo enseja remuneraçaÞo ou criação de cargos aleìm daqueles existentes na estrutura do Ministério, sendo considerada serviço puìblico relevante.

Art. 10. Compete à Alta Administração:

I - fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação do Ministério, bem como viabilizar o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados;

II - formalizar e aprovar a Política de Segurança da Informação do Ministério, bem como suas alterações e atualizações; e

III - promover a cultura de segurança da informação.

Art. 11. Compete ao Subcomitê de Governança Digital e Segurança da Informação (SGD-SI), além das competências definidas em seu ato de instituição, referenciado no § 1º do artigo 9º:

I - assessorar na implementação das ações de segurança da informação;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III - participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;

IV - propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;

V - deliberar sobre normas internas de segurança da informação;

VI - supervisionar e assegurar o cumprimento desta Política;

VII - avaliar as ações propostas pelo gestor de segurança da informação; e

VIII - consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão de segurança da informação.

Art. 12. Compete ao Gestor de Segurança da Informação (GSIN) do Ministério:

I - assessorar a alta administração e prestar suporte aos órgãos do Ministério na implementação desta Política;

II - fomentar e coordenar ações de capacitação e profissionalização contínua dos recursos humanos, com vistas a promover a cultura de segurança da informação no Ministério;

III - promover a ampla divulgação das políticas e normas internas de segurança da informação para todos os usuários de informações do Ministério;

IV - incentivar e coordenar estudos e pesquisas sobre novas tecnologias e seus impactos na segurança da informação;

V - identificar e propor os recursos financeiros, tecnológicos e humanos necessários para a implementação e manutenção das ações de segurança da informação;

VI - acompanhar os trabalhos das Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos constituídas;

VII - coordenar a elaboração de normas internas complementares de segurança da informação no âmbito do Ministério, bem como propor alterações, observadas as legislações vigentes;

VIII - monitorar os resultados das auditorias de segurança da informação, avaliando a eficácia das ações corretivas implementadas e propondo ajustes contínuos para melhorar a postura de segurança da organização;

IX - supervisionar a aplicação de ações corretivas e administrativas nos casos de violação da segurança da informação;

X - atuar como ponto de contato com o Departamento de Segurança da Informação (DSI) do Gabinete de Segurança Institucional da Presidência da República, em assuntos relativos à segurança da informação; e

XI - manter repositório centralizado e atualizado dos programas, políticas, normativos, instruções, planos, legislações, regulamentações e demais artefatos aplicáveis à gestão de segurança da informação do Ministério do Planejamento e Orçamento, bem como das políticas e artefatos correlatos desenvolvidos pelo próprio Ministério e suas unidades.

Parágrafo único. O papel de Gestor de Segurança da Informação será exercido pelo Coordenador de Tecnologia da Informação e Comunicação, da Secretaria de Administração e Gestão Estratégica da Secretaria-Executiva do Ministério do Planejamento e Orçamento, ou seu substituto legal, em seus impedimentos, afastamentos e vacância.

Art. 13. Compete às unidades de segurança da informação das secretarias, além das atribuições dispostas na legislação vigente, desempenhar ações para implementação e melhoria continua dos controles e medidas de privacidade e segurança da informação no seu âmbito de atuação, por meio da articulação com as respectivas unidades organizacionais pertinentes, em consonância com o disposto na Portaria SGD/MGI nº 852, de 28 de março de 2023, que institui o Programa de Privacidade e Segurança da Informação, bem como conhecer, cumprir e fazer cumprir esta Política e as demais normas específicas de segurança da informação do Ministério.

Art. 14. Compete aos Gestores de unidades de Tecnologia da Informação e Comunicação, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Portaria SGD/ME nº 778, de 4 de abril de 2019, 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.

Art. 15. Compete ao Encarregado pelo Tratamento de Dados Pessoais, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), 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.

Art. 16. Compete ao Responsável pela Unidade de Controle Interno, dentre outras atribuições dispostas na legislação vigente, apoiar, supervisionar e monitorar as atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa SFC/CGU nº 3, de 9 de junho de 2017.

Art. 17. Compete às Equipes de Prevenção, Tratamento Resposta a Incidentes Cibernéticos (ETIR), no seu âmbito de atuação:

I - facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos;

II - monitorar as redes computacionais;

III - detectar e analisar ataques e intrusões;

IV - tratar incidentes de segurança da informação;

V - identificar vulnerabilidades e artefatos maliciosos;

VI - recuperar sistemas de informação; e

VII - promover a cooperação com outras equipes, e participar de fóruns e redes relativas à segurança da informação.

Parágrafo único. A composição, estrutura, recursos e funcionamento das Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos serão definidos em ato da autoridade competente, de acordo com a legislação vigente.

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

Art. 18. Os ativos de informação e recursos operacionais, computacionais e de comunicação gerenciados, oferecidos ou utilizados pelo Ministério são destinados ao uso profissional para as atividades relacionadas ao Ministério.

§ 1º Os ativos e recursos citados no caput são passíveis de monitoramento e auditoria, devendo ser implementados e mantidos, sempre que possível, mecanismos que permitam a sua rastreabilidade.

§ 2º É vedada a utilização dos ativos de informação e recursos operacionais, computacionais e de comunicação para acesso, guarda e divulgação de material incompatível com ambiente do serviço, que viole direitos autorais ou que infrinja a legislação vigente.

Art. 19. Ações que provoquem quebras e violações de privacidade e segurança da informação, ou que violem esta Política e seus instrumentos complementares, devem ser apuradas e são passíveis de sanções civis, penais e administrativas, nos termos da legislação vigente.

Art. 20. Esta Política e as normas e os procedimentos de segurança da informação a ela associados deverão ser amplamente divulgados, bem como devem ser promovidos treinamentos regulares em segurança da informação.

Parágrafo único. Os treinamentos devem ser adequados às responsabilidades dos colaboradores.

Art. 21. Esta Política deverá ser revisada periodicamente para refletir mudanças no ambiente do Ministério, nos riscos à segurança da informação e nas melhores práticas.

Art. 22. As normas complementares necessárias à implementação do estabelecido nesta Política devem ser instituídas pela Estrutura de Gestão de Segurança da Informação.

Art. 23. Casos omissos sobre temas tratados por esta Política serão submetidos ao Subcomitê de Governança Digital e Segurança da Informação.

Art. 24. Esta Portaria entra em vigor na data de sua publicação.

SIMONE TEBET