PORTARIA Nº 372, DE 13 DE NOVEMBRODE 2017

Institui a Política de Segurança da Informação e Comunicações do Ministério do Planejamento, Desenvolvimento e Gestão.

O **MINISTRO DE ESTADO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO**, no uso da atribuição que lhe confere o art. 87, parágrafo único, inciso II da Constituição Federal, tendo em vista o disposto no art. 5º, inciso VII, da Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, na Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016 e nos arts. 1º e 2º da Portaria MP nº 150, de 4 de maio de 2016, que estabelece o Programa de Integridade do Ministério do Planejamento, Desenvolvimento e Gestão, resolve:

Art. 1º Instituir a Política de Segurança da Informação e Comunicações - POSIC do Ministério do Planejamento, Desenvolvimento e Gestão - MP.

CAPÍTULO I DO OBJETIVO E ABRANGÊNCIA

Art. 2º A POSIC tem por objetivo instituir princípios e diretrizes de Segurança da Informação e Comunicações - SIC no âmbito do MP, com o propósito de limitar a exposição ao risco a níveis aceitáveis e garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações e comunicações que suportam os objetivos estratégicos deste Ministério.

Art. 3º Para os efeitos dessa portaria, considera-se:

I - ativos de informação: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, os processos de negócio, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

II - gestão de ativos de informação: processo abrangente de gestão que inventaria e mapeia os ativos de informação institucionais, identificando, no mínimo e de forma inequívoca, seu conjunto completo de informações básicas (nome, descrição e localização), seus respectivos responsáveis (proprietários e custodiantes), seus requisitos legais e de negócio, sua classificação, sua documentação, seu ciclo de vida, seus riscos associados e seus controles de SIC implementados, bem como os outros ativos de informação relacionados;

III - gestão de continuidade dos negócios: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio caso essas ameaças se concretizem, de forma a fornecer uma estrutura para que se desenvolva uma resiliência organizacional capaz de recuperar perdas de ativos de informação a um nível aceitável préestabelecido, por intermédio de ações de prevenção, resposta e recuperação, de forma a salvaguardar os interesses das áreas envolvidas, a reputação, a marca da organização e suas atividades de valor agregado;

IV - gestão de segurança da informação e comunicações - GSIC: processo abrangente de gestão que desenvolve ações e métodos que visam a integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança

orgânica e segurança organizacional aos processos institucionais estratégicos, táticos e operacionais, não se

limitando ao âmbito da tecnologia da informação e comunicações; e

V - plano diretor de SIC: documento que estipula, para um período mínimo de 1 (um) ano, objetivos específicos, bem como seus indicadores e metas, com a finalidade de orientar e fazer cumprir a atuação das áreas acerca das ações necessárias de GSIC.

Art. 4º Esta POSIC e suas eventuais normas complementares aplicam-se aos órgãos de assistência direta e imediata do Ministro de Estado e aos órgãos específicos singulares do MP, conforme estabelecido na Estrutura Regimental do Ministério, abrangendo os servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e a quem, de alguma forma, tenha acesso aos ativos de informação da organização.

Art. 5º Os princípios e diretrizes gerais desta POSIC também se aplicam às entidades vinculadas ao MP e a quaisquer relacionamentos com outros órgãos e entidades públicos ou privados.

CAPÍTULO II DOS PRINCÍPIOS

Art. 6º O conjunto de documentos que compõem esta POSIC deverá guiar-se pelos seguintes princípios de segurança da informação e comunicações:

I - segregação de função: funções de planejamento, execução e controle devem ser

segregadas, de forma a atender aos objetivos institucionais e reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos;

II - menor privilégio: pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa;

III - auditabilidade: todos os eventos significantes dos processos e sistemas devem ser

rastreáveis até o evento inicial, identificando, inclusive, o responsável pelo seu acontecimento;

IV - mínima dependência de segredos: os controles de SIC devem ser efetivos, ainda que a ameaça saiba de suas existências e do seu funcionamento;

V - controles automáticos: deverão ser utilizados, sempre que possível, controles de

segurança automáticos, especialmente aqueles controles que dependem da vigilância humana e do comportamento humano;

VI - resiliência: os processos, sistemas e controles devem ser projetados para que possam resistir ou se recuperar dos efeitos de um desastre;

VII - defesa em camadas: controles devem ser desenhados em camadas ou níveis, de

tal forma que, se uma camada de controle falhar, exista um tipo diferente de controle em outra camada ou nível para prevenir a vulnerabilidade de segurança;

VIII - exceção aprovada: exceções à POSIC devem sempre ser documentadas e ter aprovação superior; e

IX - substituição da segurança em situações de emergência: controles de segurança

devem ser desconsiderados somente de formas predeterminadas e seguras, devendo existir procedimentos e controles alternativos previamente elencados para minimizar o nível de risco em situações de emergência.

CAPÍTULO III DAS DIRETRIZES GERAIS

Art. 7º O modelo de GSIC do MP deverá ser integrado e suportado pelos subsídios gerados pela Gestão de Riscos, Gestão de Ativos, Gestão de Incidentes, Gestão de Continuidade de Negócio e Gestão de Conformidade, em consonância com o especificado nas diretrizes desta POSIC.

Art. 8º A GSIC deve suportar a tomada de decisões, bem como realizar a gestão de conhecimento e de recursos por meio da utilização eficiente e eficaz dos ativos, possibilitando alcançar os objetivos estratégicos do MP, assim como otimizar seus investimentos.

Art. 9º As ações de SIC devem considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, os requisitos legais, a estrutura e a finalidade do MP.

Art. 10. Os custos associados à GSIC deverão ser compatíveis com os custos dos ativos que se deseja proteger.

Art. 11. As normas, procedimentos, manuais e metodologias de SIC do MP devem considerar, subsidiariamente, normas e padrões aceitos no mercado como referência nos processos de gestão e governança de SIC e devem estipular mecanismos que garantam a orientação à conformidade dos controles de SIC associados, inclusive sua auditabilidade.

Art. 12. Deve ser estabelecida a integração e sinergia entre as instâncias e estruturas de supervisão e apoio definidas nesta POSIC e aquelas definidas em outras políticas do MP, por meio de modelos de relacionamento que considerem e compartilhem, quando possível, as competências, responsabilidades, informações e as próprias estruturas.

SEÇÃO I DA GESTÃO DE RISCOS

Art. 13. A Estrutura de SIC do MP deverá estabelecer metodologia que possibilite a identificação, a quantificação, a priorização, o tratamento, a comunicação e a monitoração periódica dos riscos.

Art. 14. As unidades administrativas do MP, com apoio da Estrutura de SIC, deverão implementar e executar as atividades de gestão dos riscos de segurança da informação e comunicações associados aos ativos de informação sob sua responsabilidade;

Art. 15. Os riscos de SIC deverão ser considerados na contratação de serviços terceirizados, sendo os gestores das unidades administrativas e dos ativos relacionados, gestores e fiscais de contrato, bem como os fornecedores e custodiantes os responsáveis por manter os níveis apropriados de segurança da informação na entrega dos serviços.

Art. 16. As normas e procedimentos do MP devem considerar controles para a troca de informações, tanto internamente quanto externamente, de forma a manter o nível adequado de segurança da informação e comunicações.

SEÇÃO II DA GESTÃO DE ATIVOS

Art. 17. A Estrutura de SIC do MP deve instituir normas e procedimentos que garantam a adequada gestão dos ativos de informação do Ministério, em conjunto com as unidades responsáveis pelos respectivos ativos.

Art. 18. Ações e controles específicos de segurança deverão garantir a proteção

adequada dos ativos de informação do MP, em níveis compatíveis ao seu grau de importância para a consecução das atividades e objetivos estratégicos do órgão.

Art. 19. Os ativos de informação devem ser associados a controles de segurança implementados independentemente do meio em que se encontram, devendo ser protegidos contra divulgação, modificações, remoção ou destruição não autorizadas.

Art. 20. As pessoas que possuem acesso aos ativos de informação da organização devem ser periodicamente conscientizadas, capacitadas e sensibilizadas em assuntos de segurança e de tratamento da informação.

Art. 21. Os processos e atividades que sustentam os serviços críticos disponibilizados pelo MP devem ser protegidos de forma a garantir a disponibilidade, integridade, autenticidade e confidencialidade das informações e comunicações.

SEÇÃO III DA GESTÃO DA CONTINUIDADE DO NEGÓCIO

Art. 22. A Estrutura de SIC do MP, em conjunto com as áreas responsáveis pelos ativos de informação do Ministério, deverão instituir normas, procedimentos e controles que estabeleçam a gestão de continuidade do negócio, a fim de minimizar os impactos decorrentes de eventos que causem a indisponibilidade sobre os serviços do MP.

SEÇÃO IV DA GESTÃO DE INCIDENTES

Art. 23. Os incidentes de segurança da informação devem ser identificados, monitorados, comunicados e devidamente tratados, em tempo hábil, pelas áreas responsáveis pelos respectivos ativos de informação impactados, de forma a garantir a continuidade das atividades e a não intervenção no alcance dos objetivos estratégicos do MP, sem prejuízo de sua comunicação à Estrutura de SIC do MP.

SEÇÃO V DA CONFORMIDADE

Art. 24. O cumprimento desta POSIC deverá ser avaliado periodicamente, por meio de verificações de conformidade realizadas com o apoio das câmaras técnicas permanentes do Subcomitê de Gestão de SIC do MP.

Art. 25. Os controles de SIC devem ser analisados criticamente e verificados em períodos regulares pela Estrutura de SIC do MP, tendo por base a conformidade com políticas, padrões, normas, ferramentas, manuais de procedimentos e outros documentos pertinentes.

Art. 26. A Estrutura de SIC do MP deve instituir processos de análise e tratamento de conformidade, visando garantir o atendimento das leis, regulamentos e normas que regem as atividades no âmbito da Administração Pública Federal.

CAPÍTULO IV DA ESTRUTURA DE SIC E SUAS RESPONSABILIDADES

Art. 27. A SIC é disciplina fundamental da boa governança corporativa, sendo de responsabilidade do Ministro de Estado do Planejamento, Desenvolvimento e Gestão.

Art. 28. Para assessorar o Ministro de Estado do Planejamento, Desenvolvimento e Gestão nas atividades de definição e implementação de diretrizes, políticas, normas e procedimentos relativos à SIC, fica instituída a Estrutura de SIC do MP, com atribuições definidas nesta POSIC.

Art. 29. A Estrutura de SIC deverá institucionalizar um modelo de GSIC para o MP capaz de apoiar os diversos níveis hierárquicos do Ministério e seus órgãos no objetivo de integrar os controles e processos de SIC aos processos organizacionais existentes.

Parágrafo único. A participação na referida estrutura e eventuais grupos de trabalho

associados não enseja remuneração de qualquer espécie ou quaisquer criações de cargos além daqueles já existentes na estrutura regimental do MP, sendo considerada serviço público relevante.

Art. 30. A Estrutura de SIC do MP é constituída por:

I - Comitê de Gestão Estratégica - CGE;

II - Subcomitê de Gestão de SIC - SGSIC;

III - Unidades de Gestão de SIC; e

IV - Comissões de SIC.

Parágrafo único. Os responsáveis por presidir ou coordenar as instâncias que formam a referida Estrutura de SIC deverão garantir, em consonância com suas atribuições específicas, o cumprimento do disposto no capítulo III desta portaria e o efetivo desempenho das competências da respectiva instância.

Art. 31. O CGE é a instância colegiada constituída como último nível para discussão de questões relativas à SIC, com caráter deliberativo.

Parágrafo único. O regimento interno do CGE deverá ser aprovado tendo em vista os dispositivos necessários para a sua atuação nos assuntos relativos à SIC, sem prejuízo das atribuições e competências definidas na referida portaria e em outros instrumentos legais.

Art. 32. No âmbito da POSIC, compete ao CGE, em consonância com suas demais atribuições:

I - estabelecer os princípios estratégicos e as diretrizes de SIC e assegurar os recursos financeiros, materiais e humanos necessários ao seu cumprimento, alinhados aos objetivos institucionais do MP e ao arcabouço legal-normativo ao qual o Ministério está subordinado;

II - aprovar o Plano Diretor de SIC e o Programa Orçamentário de SIC, bem como monitorar sua execução; e

III - deliberar sobre proposta de alteração desta POSIC, após parecer técnico de grupo de trabalho específico do SGSIC, submetendo a proposta à aprovação do Ministro de Estado do Planejamento, Desenvolvimento e Gestão.

Art. 33. O SGSIC é a instância gerencial colegiada de apoio ao CGE do MP e será constituído:

I - pelo Gestor de SIC do MP, que presidirá o comitê;

II - pelos Coordenadores de SIC dos órgãos específicos singulares do MP; e

III - pelo Coordenador de SIC da Secretaria Executiva.

§ 1º O SGSIC do MP deverá ser assessorado em suas atividades por câmaras técnicas permanentes, que deverão tratar, no mínimo, dos seguintes temas:

a) gestão de riscos de SIC;

b) tratamento e resposta a incidentes de SIC; e

c) conformidade em SIC.

§ 2º O funcionamento do SGSIC e a composição e funcionamento de suas câmaras técnicas permanentes serão regulados por regimento interno, que deverá ser aprovado em reunião do subcomitê.

§ 3º As entidades vinculadas ao MP deverão designar representantes para compor o SGSIC, os quais deverão ter atribuições compatíveis com as de coordenação de SIC na entidade em questão.

Art. 34. Compete ao SGSIC do MP:

I - supervisionar a implementação da POSIC no âmbito do MP e seus órgãos, por meio da execução do Plano de SIC e do Programa Orçamentário de SIC;

II - discutir e aprovar, em caráter deliberativo, metodologias, normas complementares, normas operacionais e manuais de procedimentos alinhados às diretrizes desta POSIC.

III - avaliar, revisar e analisar criticamente a POSIC e suas normas complementares, visando a sua aderência aos objetivos institucionais do MP;

IV - assessorar tecnicamente o Comitê de Gestão Estratégica do MP nos assuntos relativos à SIC;

V - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC;

VI - solicitar apurações quando da suspeita de ocorrências de quebras de SIC;

VII - monitorar e avaliar a execução do Plano de SIC e do Programa Orçamentário deSIC vigentes, bem como propor e promover os ajustes cabíveis;

VIII - elaborar o Plano Diretor de SIC e o Programa Orçamentário de SIC para o ano seguinte e submetê-los à aprovação do Comitê de Gestão Estratégica do MP;

IX - garantir a infraestrutura necessária ao funcionamento de suas câmaras técnicas permanentes, bem como prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos seus membros;

X - promover a cultura de segurança da informação e comunicações, coordenando, com o apoio das demais unidades e órgãos pertinentes, as ações permanentes de divulgação, treinamento, educação e conscientização dos usuários em relação aos conceitos e às práticas de SIC, em toda a sua abrangência; e

XI - definir e atualizar seu regimento interno.

§ 1º As normas complementares, normas operacionais e os manuais de procedimentos deverão tratar de um tema específico e terão validade para todo o MP.

§ 2º As normas complementares e operacionais e os manuais de procedimentos

aprovados pelas Comissões de SIC dos órgãos do MP terão precedência de aplicação, no âmbito dos respectivos órgãos, em relação às normas complementares e operacionais e os manuais de procedimentos aprovados no Subcomitê de Gestão de SIC, desde que alinhados à POSIC.

Art. 35. As Unidades de Gestão de SIC são grupos técnicos de caráter obrigatório e permanente, presentes em cada um dos órgãos específicos singulares e na Secretaria Executiva do MP, compostos, no mínimo, por três servidores de múltiplas áreas do órgão, capacitadas periodicamente em gestão de riscos, gestão de ativos, gestão de continuidade de negócios e gestão de incidentes.

§ 1º O titular do órgão designará os membros da respectiva Unidade de Gestão de SIC.

§ 2º Na medida do possível, a respectiva Unidade de Gestão de SIC deverá compartilhar seus membros, estrutura e responsabilidades com eventuais outras unidades de supervisão técnica de gestão definidas em outras políticas do MP.

§ 3º As Unidades de Gestão de SIC serão coordenados pelo Coordenador de SIC do órgão correspondente.

Art. 36. Compete à Unidade de Gestão de SIC:

I - apoiar os atores com responsabilidades nos processos do órgão, para que eles possam implementar os controles de segurança em gestão de riscos, gestão de ativos, gestão de continuidade de negócios e gestão de incidentes;

II - recolher evidências da implementação dos controles de segurança da gestão de riscos, gestão de ativos, gestão de continuidade de negócios e gestão de incidentes dos processos da organização;

III - elaborar relatório de monitoramento da gestão de risco, gestão de ativos, gestão de continuidade de negócios e gestão de incidentes no órgão;

IV - estimar necessidade de treinamento em gestão de riscos, gestão de ativos, gestão de continuidade de negócios e gestão de incidentes para os servidores do órgão; e

V - elaborar e executar, no âmbito do órgão, processos que garantam a Gestão deContinuidade de Negócio, conforme legislação pertinente.

Art. 37. As Comissões de SIC são instâncias colegiadas de caráter obrigatório presentes em cada um dos órgãos específicos singulares e na Secretaria Executiva do MP, às quais compete, no âmbito do respectivo órgão:

I - discutir e aprovar eventuais normas operacionais complementares e manuais de procedimentos relativos à SIC, em conformidade com esta POSIC; e

II - acompanhar e monitorar as atividades da respectiva Unidade de Gestão de SIC, garantindo os recursos necessários ao seu funcionamento.

§ 1º As Comissões de SIC serão compostas, no mínimo, pelos seguintes membros:

I - o Coordenador de SIC do órgão, que coordenará a comissão;

II - pelo menos um membro da respectiva Unidade de Gestão de SIC do órgão;

III - um servidor do Gabinete do titular do órgão; e

IV - um representante de cada diretoria ou unidade equivalente da estrutura do órgão.

§ 2º O titular do órgão designará os membros da Comissão de SIC e seu funcionamento será disciplinado em regimento interno, que deverá ser discutido e aprovado em reunião da comissão.

§ 3º Na medida do possível, as atribuições da Comissão de SIC, no âmbito do órgão, deverão ser desempenhadas por instâncias de gestão previamente existentes, desde que sua composição, competências e regimento interno sejam formalmente compatibilizados ao estipulado neste artigo.

Art. 38. O Gestor de SIC será designado pelo Ministro de Estado do Planejamento, Desenvolvimento e Gestão dentre os servidores do seu quadro, que detenham conhecimento em SIC em nível adequado para o exercício da função, tendo como atribuições:

I - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

II - propor recursos necessários às ações de segurança da informação e comunicações;

III - presidir e coordenar o SGSIC, convocar suas reuniões e representá-lo perante oComitê de Gestão Estratégica do MP;

IV - realizar e acompanhar estudos e novas tecnologias, no tocante a possíveis impactos na segurança da informação e comunicações;

V - manter contato direto com o Departamento de Segurança da Informação eComunicações do Gabinete de Segurança Institucional da Presidência da República, para o trato de assuntos relativos à segurança da informação e comunicações;

VI - propor normas relativas à SIC; e

VII - acompanhar e monitorar as atividades das câmaras técnicas permanentes doSGSIC.

Art. 39. Os Coordenadores de SIC deverão estar presentes em cada um dos órgãos específicos singulares e na Secretaria Executiva do MP, sendo designados pelos respectivos titulares dentre os servidores que ali ocupem cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS ou Função Comissionada do Poder Executivo - FCPE, de nível 4 ou superior e que detenham conhecimento em SIC em nível adequado para o exercício da função, com as seguintes atribuições:

I - implementar as diretrizes da POSIC e as decorrentes normas complementares e manuais de procedimentos no âmbito do respectivo órgão;

II - coordenar a respectiva Unidade de Gestão de SIC;

III - coordenar a respectiva Comissão de SIC do órgão, convocando suas reuniões e informando ao SGSIC a aprovação de eventuais normas e procedimentos por parte da comissão;

IV - representar o órgão no SGSIC do MP; e

V - consolidar estatísticas sobre a situação da Gestão de SIC do órgão - inclusive relacionadas ao Plano Diretor de SIC e ao Programa Orçamentário de SIC - para comunicação e apresentação à respectiva Comissão de SIC e ao SGSIC, quando solicitado.

Art. 40. A Estrutura de SIC do MP deverá estipular e implementar mecanismos que apoiam e garantam o comprometimento dos recursos humanos na implementação das diretrizes desta POSIC.

Parágrafo único. Os servidores do MP responsáveis pelos processos da organização deverão integrá-los aos processos e controles de SIC, acionando, sempre que necessário, a Unidade de Gestão de SIC do respectivo órgão, para prestar apoio.

CAPÍTULO V DAS PENALIDADES

Art. 41. Ações que violem esta POSIC ou que quebrem os controles de segurança da informação e comunicações serão passíveis de sansões civis, penais e administrativas, conforme a legislação em vigor.

CAPÍTULO VI DAS DISPOSIÇÕES FINAIS

Art. 42. A POSIC e os documentos dela derivados deverão ser revisados sempre que mudanças significativas na estrutura do MP ocorrerem ou quando alterações em normas e outras políticas forem aprovadas, ou ainda periodicamente, conforme legislação vigente, sendo atualizados quando necessário.

Art. 43. A POSIC e as normas e os procedimentos de SIC a ela associados deverão ser amplamente divulgados.

Art. 44. O Gestor de SIC e os Coordenadores de SIC da Secretaria Executiva e dos órgãos específicos singulares do MP deverão ser designados em até 30 (trinta) dias após a publicação desta Portaria e informados à Secretaria Executiva do MP.

Art. 45. O Subcomitê de Gestão de SIC deverá se reunir em até 30 (trinta) dias após a formalização de todas as designações de que trata o art. 44 e deverá ter seu regimento interno aprovado em até 90 (noventa) dias da data da primeira reunião.

Art. 46. As Unidades de Gestão de SIC e as Comissões de SIC deverão ser constituídas no prazo de 15 (quinze) dias após a designação do Coordenador de SIC do órgão.

Art. 47. Esta Portaria entra em vigor na data de sua publicação.

Art. 48. Fica revogada a Portaria MP nº 27, de 3 de fevereiro de 2012.

DYOGO HENRIQUE DE OLIVEIRA

PUBLICADA NO DOU
DE 16/11/2017,
SEÇÃO 1, PÁGINAS 115 A 116