INSTRUÇÃO NORMATIVA Nº 1, DE 27 DE MAIO DE 2020

Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, no uso das atribuições que lhe conferem o art. 87 da Constituição, a Lei nº 13.844, de 18 de junho de 2019, e o Decreto nº 9.668, de 2 de janeiro de 2019, considerando o disposto no art. 12 do Decreto nº 9.637, de 26 de dezembro de 2018, e em cumprimento ao Decreto nº 10.139, de 28 de novembro de 2019 resolve:

Art. 1º Aprovar a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 2º A Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal dispõe sobre as orientações para gestão de segurança da informação que deverão ser observadas e implementadas pelos órgãos e pelas entidades da administração pública federal, direta e indireta, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional.

Art. 3º Para os fins do disposto nesta Instrução Normativa, a segurança da informação abrange:

I - a segurança cibernética;

II - a defesa cibernética;

III - a segurança física;

IV - a proteção de dados organizacionais; e

V - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

CAPÍTULO II

DAS REFERÊNCIAS NORMATIVAS DE SEGURANÇA DA INFORMAÇÃO

Art. 4º Para o planejamento da gestão da segurança da informação, cabe aos órgãos e às entidades da administração pública federal observar, sem prejuízo das demais normas em vigor:

I - o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

II - a Resolução SE/GSI nº 1, de 11 de setembro de 2019, que aprova o Regimento Interno do Comitê Gestor de Segurança da Informação;

III - a Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário

IV de Segurança da Informação;

V - o Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética; e

VI - as instruções normativas relacionadas à segurança da informação,

VII- publicadas pelo Gabinete de Segurança Institucional da Presidência da República.

Seção I

Da Política Nacional de Segurança da Informação

Art. 5º Devem ser considerados no planejamento da gestão da segurança da informação os seguintes aspectos da Política Nacional de Segurança da Informação, instituída por meio do Decreto nº 9.637, de 2018:

I - a abrangência da segurança da informação;

II - os objetivos;

III - os instrumentos;

IV - a instituição e as competências do Comitê Gestor de Segurança da Informação;

V - as competências do Gabinete de Segurança Institucional da Presidência da República;

VI - as competências do Ministério da Defesa;

VII- as competências da Controladoria-Geral da União; e

VIII - as competências dos demais órgãos e das entidades da administração pública federal.

Seção II

Do Glossário de Segurança da Informação

Art. 6º Os órgãos e as entidades da administração pública federal deverão utilizar o Glossário de Segurança da Informação, aprovado pelo Gabinete de Segurança Institucional da Presidência da República por meio da Portaria GSI/PR nº 93, de 26 de

setembro de 2019, como referência na elaboração de normativos internos afetos à segurança da informação e de trabalhos correlatos.

Art. 7º O Glossário de Segurança da Informação, sempre que possível, será

atualizado pelo Gabinete de Segurança Institucional da Presidência da República, devendo os órgãos e as entidades da administração pública federal enviar, a qualquer tempo, contribuições e sugestões para seu aperfeiçoamento.

Seção III

Da Estratégia Nacional de Segurança Cibernética

Art. 8º Devem ser considerados no planejamento da gestão da segurança da informação, em especial, os seguintes aspectos da Estratégia Nacional de Segurança Cibernética, aprovada pelo Decreto nº 10.222, de 2020:

I - os objetivos estratégicos; e

II - as ações estratégicas.

CAPÍTULO III

DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Art. 9º É obrigatório a todos os órgãos e as entidades da administração pública federal possuir uma Política de Segurança da Informação, implementada a partir da formalização e aprovação por parte da autoridade máxima da instituição, com o objetivo de estabelecer diretrizes, responsabilidades, competências e subsídios para a gestão da segurança da informação.

Parágrafo único. A autoridade máxima do órgão ou da entidade é responsável por garantir os recursos necessários para a execução da Política de Segurança da Informação no âmbito de sua organização.

Art. 10. A Política de Segurança da Informação deve ser elaborada sob a coordenação do Gestor de Segurança da Informação do órgão ou entidade, com a participação do Comitê de Segurança da Informação interno ou estrutura equivalente.

Parágrafo único. Cabe ao Gestor de Segurança da Informação promover, com apoio da alta administração, a ampla divulgação da Política, das normas internas de segurança da informação e de suas atualizações, de forma ampla e acessível, a todos os servidores, aos usuários e aos prestadores de serviço, a fim de que esses tomem conhecimento de tais instrumentos.

Art. 11. A elaboração da Política de Segurança da Informação deve levar em consideração a natureza e a finalidade do órgão ou da entidade e estar alinhada ao seu planejamento estratégico.

Art. 12. A Política de Segurança da Informação deverá ser composta, no mínimo, pelos seguintes itens:

I - escopo: descreve o objetivo e a abrangência da Política, definindo o limite dentro do qual as ações de segurança da informação serão desenvolvidas no órgão ou na entidade;

II - conceitos e definições: relaciona e descreve os conceitos e definições a serem utilizados na Política do órgão ou da entidade que possam gerar dificuldade de interpretação ou ambiguidade, devendo ser utilizadas as definições contidas no Glossário de Segurança da Informação, aprovado pelo Gabinete de Segurança Institucional da Presidência da República;

III - princípios: relaciona os princípios que regem a segurança da informação no órgão ou na entidade;

IV - diretrizes gerais: estabelece diretrizes sobre a implementação, no mínimo, dos seguintes temas:

a) Tratamento da Informação;

b) Segurança Física e do Ambiente;

c) Gestão de Incidentes em Segurança da Informação;

d) Gestão de Ativos;

e) Gestão do Uso dos Recursos Operacionais e de Comunicações, como: e-mail, acesso à internet, mídias sociais, computação em nuvem, dentre outros;

f) Controles de Acesso;

g) Gestão de Riscos;

h) Gestão de Continuidade; e

i) Auditoria e Conformidade.

V - competências: define as atribuições e as responsabilidades dos envolvidos na estrutura de gestão de segurança da informação;

VI - penalidades: estabelece as consequências e as penalidades para os casos de violação da Política de Segurança da Informação ou de quebra de segurança, de acordo com as normas já existentes no ordenamento jurídico vigente sobre penalidades ao servidor público federal relativas ao assunto; e

VII- política de atualização: estabelece a periodicidade máxima para a revisão da Política de Segurança da Informação e dos respectivos instrumentos normativos.

§ 1º A periodicidade para a revisão da Política de Segurança da Informação não deve exceder 4 (quatro) anos.

§ 2º A Política de Segurança da Informação, quando necessário, deve ser complementada por normas, metodologias e procedimentos.

Art. 13. A elaboração e a adoção de uma Política de Segurança da Informação interna evidenciam o comprometimento da alta administração com vistas a prover diretrizes estratégicas, responsabilidades, competências e apoio para implementar a gestão da segurança da informação em sua organização.

CAPÍTULO IV

DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA

Art. 14. Ao Gabinete de Segurança Institucional da Presidência da República compete a publicação de atos normativos sobre Segurança da Informação, que devem abordar os principais aspectos a serem observados no planejamento de ações relacionadas a esse tema no âmbito dos órgãos e das entidades da administração pública federal.

Parágrafo único. A adoção dos controles gerais de segurança da informação estabelecidos pelo Gabinete de Segurança Institucional da Presidência da República é de cumprimento obrigatório para a alta administração dos órgãos e das entidades da administração pública federal.

CAPÍTULO V

DOS ÓRGÃOS E DAS ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Art. 15. Além das obrigações já dispostas nesta Instrução Normativa, compete aos órgãos e às entidades da administração pública federal, direta e indireta, em seu âmbito de atuação:

I - designar um gestor de segurança da informação interno, indicado pela alta administração do órgão ou da entidade;

II - instituir Comitê de Segurança da Informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à Política Nacional de Segurança da Informação;

III - promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação;

IV - instituir e implementar Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR, que constituirá a rede de equipes, integrada pelos órgãos e pelas entidades da administração pública federal, coordenada pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo do Gabinete de Segurança Institucional da Presidência da República; (Redação dada pela Instrução Normativa nº 2, de 2020)

V - coordenar e executar as ações de segurança da informação no âmbito de sua atuação;

VI - consolidar e analisar os resultados dos trabalhos de auditoria sobre gestão de segurança da informação; e

VII- aplicar as ações corretivas e administrativas cabíveis, nos casos de violação da segurança da informação.

CAPÍTULO VI

DA ESTRUTURA PARA A GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Art. 16. De forma a estruturar a gestão da segurança da informação, os órgãos e entidades da administração pública federal deverão designar ou instituir, ao menos:

I - o Gestor de Segurança da Informação;

II - o Comitê de Segurança da Informação ou estrutura equivalente; e

III - uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) ou estrutura equivalente. (Redação dada pela Instrução Normativa nº 2, de 2020)

Art. 17. Os órgãos e as entidades da administração pública federal deverão utilizar os guias metodológicos que serão disponibilizados pelo Gabinete de Segurança Institucional da Presidência da República em seu sítio eletrônico, para fins de implementação de ações relacionadas à gestão da segurança da informação.

Seção I (Redação dada pela Instrução Normativa nº 9, de 2026)

Do Gestor de Segurança da Informação

Art. 18. Compete aos órgãos e às entidades da administração pública federal a designação do gestor de segurança da informação, observados os seguintes requisitos cumulativamente:

I - ser servidor ou empregado público civil ocupante de cargo efetivo ou militar das Forças Armadas;

II - ser ocupante de Cargo Comissionado Executivo – CCE ou Função Comissionada Executiva – FCE de nível 15, equivalente ou superior, ou oficial general, na hipótese de militar das Forças Armadas;

III - não ser o responsável pela unidade de tecnologia da informação ou seu subordinado, salvo quando não houver no órgão ou na entidade outro servidor, empregado ou militar apto ao exercício do encargo, hipótese em que o ato de designação deverá conter justificativa formal e fundamentada sobre eventual conflito de competências; e

IV - possuir conhecimentos ou estar em processo de formação em segurança da informação.

§1º O substituto do gestor de segurança da informação deverá atender aos requisitos dispostos nos incisos I, III e IV do caput, e ser ocupante de Cargo Comissionado Executivo – CCE ou Função Comissionada Executiva – FCE de nível 13, equivalente ou superior, ou oficial superior do último posto, na hipótese de militar das Forças Armadas.

§2º Em órgãos e entidades em que o dirigente máximo seja ocupante de Cargo Comissionado Executivo – CCE ou Função Comissionada Executiva – FCE de nível igual ou inferior a 15, ou equivalente, é permitida a designação de servidores ocupantes de CCE ou FCE de nível igual ou superior a 13 ao titular, e de nível igual ou superior a 10 ao substituto, observados os demais requisitos dispostos nos incisos I, III e IV do caput.

§3º O Gabinete de Segurança Institucional ofertará formações de gestores de segurança da informação para o atendimento ao requisito previsto no inciso IV do caput.

Art. 19. Ao Gestor de Segurança da Informação dos órgãos e das entidades da administração pública federal compete, no âmbito de sua atuação, exercer as seguintes atribuições:

I - coordenar as iniciativas de segurança da informação no âmbito do órgão ou da entidade ao qual representa, garantindo o cumprimento das normas internas e da legislação vigente;

II - estimular iniciativas de capacitação em temas relacionados à segurança da informação e promover ações de conscientização sobre boas práticas aos agentes públicos;

III - divulgar as normas internas de segurança da informação a todos os agentes públicos;

IV - realizar avaliações de riscos e análise dos impactos antes da adoção de tecnologias emergentes no contexto de seu órgão ou entidade;

V - planejar e propor os recursos orçamentários necessários à implementação, atualização e manutenção de iniciativas de segurança da informação;

VI - acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

VII - atuar como segunda linha de defesa no âmbito do Sistema de Controle Interno;

VIII - realizar avaliações de conformidade em relação à implementação de requisitos estabelecidos na Política Nacional de Segurança da Informação (PNSI), nas normas inferiores e na legislação aplicável à segurança da informação, e apoiar auditorias internas e externas;

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

X - cooperar com o Encarregado pelo Tratamento de Dados Pessoais nas ações relativas à segurança da informação quando envolver dados pessoais;

XI - elaborar e revisar o planejamento tático de segurança da informação, e acompanhar sua implementação;

XII - participar de fóruns especializados para obtenção de experiências e ampliação de capacidades, tanto no setor público quanto no setor privado; e

XIII - avaliar a capacidade operacional do órgão ou da entidade que representa, a fim de:

a subsidiar as decisões dos gestores superiores sobre ações de segurança da informação; e,

b emitir parecer técnico ou recomendação sobre a conveniência de integrar ou desligar-se de arranjos colaborativos de segurança da informação.

Parágrafo único. O responsável pela unidade de tecnologia da informação deverá colaborar e fornecer os subsídios necessários ao Gestor de Segurança da Informação para a execução de suas competências."

Art. 19-A. Os órgãos e as entidades da administração pública federal poderão designar servidor para o exercício de atribuições análogas às do Gestor de Segurança da Informação, no âmbito de suas unidades administrativas.

§ 1º A designação de que trata o caput não configura a criação de cargo, emprego ou função pública, mas a atribuição de responsabilidades a servidor já ocupante de cargo público, o qual passará a ser identificado, em sua respectiva unidade, como Gestor Setorial de Segurança da Informação.

§ 2º O servidor designado deverá observar os requisitos previstos nos incisos I, III e IV do art. 18 e atuará sob a governança do Gestor de Segurança da Informação titular do órgão ou entidade, ao qual deverá se reportar.

Art. 19-B. Os órgãos e as entidades da administração pública federal deverão comunicar à Secretaria de Segurança da Informação e Cibernética do Gabinete de Segurança Institucional os nomes e os dados para contato do Gestor de Segurança da Informação, titular e substituto, e de eventuais Gestores Setoriais de Segurança da Informação, sempre que houver uma nova designação.

Seção II

Do Comitê de Segurança da Informação

Art. 20. O Comitê de Segurança da Informação interno dos órgãos e das entidades da administração pública federal possui as seguintes atribuições:

I - assessorar a 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; (Redação dada pela Instrução Normativa nº 7, de 2022)

V - deliberar sobre normas internas de segurança da informação; e (Redação dada pela Instrução Normativa nº 7, de 2022)

VI - deliberar sobre as ações propostas pelo gestor de segurança da informação no parecer técnico sobre o relatório de avaliação de conformidade e encaminhar à alta administração para aprovação o processo contendo os documentos sobre a avaliação de conformidade. (Incluído pela Instrução Normativa nº 7, de 2022)

Art. 21. O Comitê de Segurança da Informação disposto no art. 20 terá a seguinte composição:

I - o gestor de segurança da informação do órgão ou da entidade; (Redação dada pela Instrução Normativa nº 7, de 2022)

II - um representante da Secretaria-Executiva ou da unidade equivalente do

III órgão ou da entidade;

IV - um representante de cada unidade finalística do órgão ou da entidade; e

V - o titular da unidade de tecnologia da informação do órgão ou da entidade.

Parágrafo único. O Comitê de Segurança da Informação será coordenado pela maior autoridade designada. (Incluído pela Instrução Normativa nº 7, de 2022)

Seção III

Da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos

Art. 22. Todos os órgãos e entidades que possuem a competência de administrar a infraestrutura de rede de sua organização deverão criar uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos. (Redação dada pela Instrução Normativa nº 2, de 2020)

§ 1º Deverá ser elaborado documento de constituição da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, o qual designará suas atribuições e seu escopo de atuação. (Redação dada pela Instrução Normativa nº 2, de 2020)

§ 2º A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos será composta, preferencialmente, por servidores públicos civis ocupantes de cargo efetivo ou militares, com capacitação técnica compatível com as atividades dessa equipe. (Redação dada pela Instrução Normativa nº 2, de 2020)

§ 3º A atuação da Equipe será regida por normativos, padrões e procedimentos técnicos exarados pelo Centro de Tratamento e Resposta de Incidentes Cibernéticos do Governo, sem prejuízo das demais metodologias e padrões conhecidos.

§ 4º As notificações enviadas pela Equipe ao Centro de Tratamento e Resposta à Incidentes Cibernéticos de Governo, bem como a troca de informações entre as Equipes existentes, devem seguir os formatos e os procedimentos que serão estabelecidos pelo Centro de Tratamento e Resposta de Incidentes Cibernéticos do Governo.

CAPÍTULO VII

DOS ATOS DE DISPOSIÇÕES TRANSITÓRIAS

Art. 23. Ficam revogados os seguintes atos normativos:

I - a Instrução Normativa GSI Nº 1, de 13 de junho de 2008;

II - a Norma Complementar nº 01, de 13 de outubro de 2008;

III - a Norma Complementar nº 02, de 13 de outubro de 2008; e

IV - a Norma Complementar nº 03, de 30 de junho de 2009.

Parágrafo único. As referidas normas preservarão seus efeitos até a entrada em vigor desta Instrução Normativa.

Art. 24. Esta Instrução Normativa entra em vigor no dia 1º de julho de 2020.

AUGUSTO HELENO RIBEIRO PEREIRA