Instrução Normativa PRODERJ/PRE Nº 2 DE 28/04/2022

Regulamenta os procedimentos de segurança da informação em soluções de Tecnologia da Informação e Comunicação - TIC a serem adotados pelos órgãos e entidades integrantes da administração direta e indireta do Poder Executivo do Estado do Rio de Janeiro.

O Presidente do Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro - PRODERJ, no uso de suas atribuições que lhe conferem as alíneas "b", "c" e "e" do inciso XVIII do art. 5º e inciso VII do art. 6º do Decreto nº 47.278, de 17 de setembro de 2020,

Considerando:

- o que consta no processo nº SEI-12/001/044587/2019;

- a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) e sua regulamentação pelo Decreto nº 43.597 , de 17 de maio de 2012;

- a Lei nº 13.709 , de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);

- a Portaria PRODERJ/PRE Nº 825, de 26 de fevereiro de 2021, que institui a Estratégia da Governança de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro - EGTIC/RJ, notadamente o art. 1º, IV, que prevê a instituição de Instruções Normativas para a efetivação da Governança de Tecnologia da Informação e Comunicação no Estado do Rio de Janeiro, bem como o art. 11, do Anexo B, que trata de ações de governança voltadas à segurança da informação e à proteção de dados;

- as competências do PRODERJ conforme as disposições do art. 2º da Lei nº 4.480, de 28 de dezembro de 2004, e as regulamentações pelo art. 5º do Decreto nº 47.278, de 17 de setembro de 2020;

- a indispensável atualização dos dispositivos legais que regulamentam a área de Tecnologia da Informação e Comunicação - TIC do Estado do Rio de Janeiro;

- a devida contribuição para a segurança do indivíduo, da sociedade e do Estado, por meio da orientação de governança e das ações de segurança da informação, observadas legislações vigentes;

- a premência em regulamentar os procedimentos de segurança que assegurarão a confidencialidade, a integridade e a disponibilidade de informações e ativos, contribuindo

para o cumprimento dos objetivos estratégicos do Estado e a melhoria da gestão do Sistema Estadual de Tecnologia da Informação e Comunicação - SETIC;

- a promoção do aperfeiçoamento das boas práticas da área de segurança da informação, estimular e fortalecer essa cultura no Estado;

- a conveniência em estabelecer conceitos e diretrizes de segurança da informação para implantar e manter processos e ações para gerenciar as ameaças aos recursos de tecnologia da informação e comunicação;

- a necessidade de fomentar a formação e a qualificação dos recursos humanos necessários à área de segurança da informação,

Resolve:

CAPÍTULO I - DAS DISPOSIÇÕES GERAIS

Art. 1º Ficam regulamentados os procedimentos a serem adotados pelos órgãos e entidades da Administração Direta e Indireta do Poder Executivo do Estado do Rio de Janeiro quanto à segurança da informação, que envolvam Tecnologia de Informação e Comunicação, na forma das disposições desta Instrução Normativa e do seu Anexo Único, com a finalidade de aprimorar a segurança da informação no âmbito da Administração Pública Estadual.

§ 1º Para os fins do disposto nesta Instrução Normativa, a segurança da informação abrange:

I - segurança cibernética;

II - defesa cibernética;

III - segurança física;

IV - proteção de dados organizacionais;

V - proteção de dados pessoais; e

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

§ 2º O Anexo Único desta Instrução Normativa dispõe, em seu item "4", acerca dos conceitos e definições pertinentes.

CAPÍTULO II - DOS PRINCÍPIOS

Art. 2º As ações de segurança da informação e comunicação previstas nesta Instrução Normativa e em seu Anexo Único serão norteadas pelos princípios constitucionais elencados no rol do art. 37 da Constituição da República Federativa do Brasil, assim como o da dignidade da pessoa humana, previsto no art. 1º, inciso III da Constituição da República, e o art. 5º da Constituição do Estado do Rio de Janeiro, também os princípios da Governança de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro, instituída pela Portaria PRODERJ/PRE nº 825, de 26 de fevereiro de 2021, bem como pela:

I - publicidade;

II - integridade;

III - disponibilidade;

IV - autenticidade;

V - confidencialidade;

VI - responsabilidade;

VII - não-repúdio; e

VIII - prevenção.

CAPÍTULO III - DAS DIRETRIZES

Seção I - Das Diretrizes Gerais

Art. 3º A informação relacionada às operações do Governo do Estado, gerada ou desenvolvida em suas dependências, durante a execução das atividades diárias de gestão, constitui ativo desta instituição, essencial à condução das operações, e, em última análise, à sua existência.

Art. 4º Os servidores, terceiros e fornecedores, em qualquer vínculo, função ou nível hierárquico no Estado, que tenham qualquer tipo de contato e/ou acesso aos recursos de tecnologia da informação e comunicação são responsáveis pela segurança, zelo e bom uso dos ativos às quais têm acesso, sejam do próprio governo, do cidadão ou de outro órgão ou entidade.

Art. 5º As instalações e equipamentos devem ser protegidos contra acessos não autorizados, devendo os órgãos e entidades estaduais implementar mecanismos de proteção que impeçam acesso indevido aos ativos tecnológicos e às áreas em que se encontram.

Art. 6º Toda informação custodiada em ativos tecnológicos nos órgãos e entidades estaduais deve possuir cópia de segurança (backup) e ser guardada em local protegido, para que não sejam alteradas, acessadas ou eliminadas indevidamente.

Art. 7º As informações que não sejam mais necessárias devem ser descartadas com segurança, conforme os procedimentos que cada órgão instituirá na forma do art. 9º desta Instrução Normativa.

Art. 8º Os usuários devem ser orientados a manter em absoluto sigilo suas senhas, sendo vedada a divulgação ou compartilhamento com terceiros a fim de preservar os ativos de tecnologia da informação.

Art. 9º Os órgãos e entidades estaduais deverão manter procedimentos de segurança da informação, com normas claras, objetivas, revisadas e divulgadas regularmente, com base nas diretrizes estabelecidas neste instrumento e nos normativos do órgão de Direção Geral do Sistema Estadual de Tecnologia da Informação e Comunicação - SETIC, para orientar a correta utilização dos recursos computacionais em suas redes.

Art. 10. Os procedimentos de segurança da informação constantes do Anexo Único desta Instrução Normativa, bem como as normas complementares previstas no art. 16, deverão ser atualizados periodicamente, sempre que algum fato relevante ou evento motive sua revisão.

Parágrafo único. A metodologia de implantação dos procedimentos de segurança da informação previstos no anexo único deste instrumento deve seguir o processo interativo de melhoria contínua, apresentado pelo modelo conhecido como "Plan-Do-Check-Act" (PDCA), ciclo Planejar, Executar, Checar e Agir, tendo como conceito:

I - planejar: processo no qual as ações de segurança da informação são definidas através da delimitação do escopo, limites, objetivos e metas, considerando os requisitos e diretrizes expedidas pela autoridade decisória de seu órgão ou entidade;

II - executar: implementar e operar as normas, controles, processos e procedimentos de segurança da informação previstos no anexo único deste instrumento;

III - checar: processo no qual os processos serão analisados através de ferramentas próprias, para verificar o desempenho das ações e se estão de acordo com o planejamento. Além disso, nessa fase que poderão ser encontrados erros ou falhas no processo;

IV - agir: etapa na qual serão executadas as ações corretivas e preventivas, com base nos resultados da checagem, visando corrigir possíveis desvios e alcançar melhoria contínua

dos procedimentos de segurança da informação previstos no Anexo Único desta Instrução Normativa.

Seção II - Das Diretrizes Específicas

Art. 11. Os órgãos e entidades estaduais, ao estabelecerem os procedimentos de segurança da informação, previstos no art. 9º, deverão contemplar minimamente o seguinte arcabouço normativo:

I - Escopo: descrever o objetivo e abrangência, definindo o limite no qual as ações de segurança da informação serão desenvolvidas no órgão ou entidade;

II - Referências legais e normativas: identificar as referências legais e normativas utilizadas para a elaboração dos seus procedimentos de segurança da informação;

III - Conceitos e definições: relacionar e descrever os conceitos e definições a serem utilizados nos procedimentos de segurança da informação do órgão ou da entidade que possam gerar dificuldade de interpretação ou ambiguidade;

IV - Princípios: relacionar os princípios que regem a segurança da informação no órgão ou entidade;

V - Diretrizes gerais: estabelecer diretrizes que orientarão o uso adequado dos ativos de segurança da informação e as medidas de segurança apropriadas, considerando, minimamente, os incisos do § 1º do art. 1º;

VI - Competências e responsabilidades: definir a estrutura para a gestão da segurança da informação em seu âmbito de atuação, compreendendo, no mínimo:

a) Gestor de Segurança da Informação, na forma do art. 17;

b) Responsável pelo Tratamento e Resposta a Incidentes, na forma do art. 18;

c) Encarregado pelo Tratamento de Dados Pessoais, na forma do art. 19.

VII - Penalidades: estabelecer as consequências e as penalidades para os casos de violação de seus procedimentos de segurança da informação ou de quebra de segurança, de acordo com as normas já existentes no ordenamento jurídico vigente relativas ao assunto; e

VIII - Atualização: estabelecer a periodicidade da revisão dos instrumentos normativos gerados a partir dos próprios procedimentos de segurança da informação.

§ 1º Os órgãos que possuírem entidades vinculadas deverão definir a abrangência dos procedimentos de segurança da informação, podendo, em casos de problemas estruturais

ou baixa maturidade, elaborar normas conjuntas com as entidades vinculadas as abrangendo.

§ 2º Cada órgão e entidade estadual deverá ter um Gestor de Segurança da Informação e um Responsável pelo Tratamento e Resposta a Incidentes, com as respectivas competências, conforme o art. 17 e art. 18 desta Instrução Normativa.

Art. 12. Para elaboração dos procedimentos de segurança da informação deverão ser acionados representantes de diferentes setores do órgão ou entidade, como, por exemplo, segurança patrimonial, tecnologia da informação e comunicação, recursos humanos e jurídicos, que deverão alinhar-se sempre à natureza, finalidade e ao planejamento estratégico do órgão ou entidade elaborador.

Art. 13. Os procedimentos de segurança da informação deverão ser aprovados pelo titular responsável pelo órgão ou entidade, com a devida publicidade e acompanhamento para a garantia da provisão dos recursos necessários à implementação da política e da cultura de segurança da informação.

Art. 14. Quaisquer pessoas que tenham contato com os recursos de tecnologia da informação e comunicação, no âmbito dos órgãos e entidades estaduais, são responsáveis por seguir as normas dos procedimentos de segurança da informação, devendo ser exigido de tais pessoas um termo de uso e responsabilidade, conforme modelo sugerido no anexo único desta instrução.

Art. 15. Os órgãos e entidades devem adotar cláusulas de segurança da informação nos contratos com terceiros, de forma a resguardar o sigilo e a confidencialidade de toda e qualquer informação constante nos seus ativos tecnológicos, com as quais os prestadores de serviços venham a ter contato.

Seção III - Das Normas Complementares

Art. 16. Com o propósito de assegurar a confidencialidade, disponibilidade e integridade dos ativos tecnológicos, o Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro - PRODERJ instituirá normas complementares a esta Instrução Normativa, a serem observadas pelos demais órgãos e entidades, para regular aspectos pontuais de segurança da informação.

§ 1º As normas complementares deverão permanecer disponíveis no Portal do SETIC, cujo link se encontra no preâmbulo do Anexo Único desta Instrução Normativa.

§ 2º Os demais órgãos da administração estadual poderão instituir normas complementares a esta Instrução Normativa conforme suas necessidades e dentro de suas competências, devendo disponibilizálas em seus portais na internet.

CAPÍTULO IV - DOS AGENTES NOS ÓRGÃOS E ENTIDADES

Seção I - Do Gestor de Segurança da Informação

Art. 17. Compete ao Gestor de Segurança da Informação dos órgãos e entidades:

I - elaborar e atualizar periodicamente os procedimentos de segurança da informação do órgão/entidade que seja responsável;

II - implementar e monitorar permanentemente os mecanismos e procedimentos relacionados à segurança da informação, com o intuito de preservar a integridade, a confidencialidade e a privacidade dos dados sob a guarda e responsabilidade dos órgãos e entidades;

III - promover a cultura de segurança da informação no âmbito de atuação do órgão ou entidade elaborador;

IV - acompanhar eventos e danos decorrentes de incidentes e eventos de segurança da informação;

V - compartilhar com os demais órgãos e entidades da Administração Pública Estadual, os eventos de segurança, após ocorrência, para fins de prevenção, bem como as eventuais soluções, para fins de replicação de conhecimentos e experiências;

VI - propor recursos necessários às ações de segurança da informação, no âmbito de atuação do seu órgão ou entidade; e

VII - indicar os responsáveis pelo tratamento de resposta a incidentes no âmbito de atuação do órgão ou entidade elaborador.

Parágrafo único. O Gestor de Segurança da Informação será designado dentre os servidores públicos civis ou militares ocupantes de cargos efetivos, desde que lotados no órgão ou entidade e com formação ou capacitação técnica compatível às suas atribuições.

Seção II - Do Responsável pelo Tratamento e Resposta a Incidentes

Art. 18. Compete ao Responsável pelo Tratamento e Resposta a Incidentes:

I - monitorar os recursos de TIC, detectar e realizar as análises dos incidentes de segurança da informação;

II - reportar ao Encarregado pelo Tratamento de Dados Pessoais os incidentes envolvendo tais dados;

III - identificar vulnerabilidades;

IV - receber e propor respostas a notificações relacionadas a incidentes de segurança da informação; e

V - coordenar e executar atividades de tratamento e resposta a eventos de segurança da informação.

Parágrafo único. O Responsável pelo Tratamento e Resposta a Incidentes será designado dentre os servidores públicos civis ou militares ocupantes de cargos efetivos, desde que lotados no órgão ou entidade e com formação ou capacitação técnica compatível às suas atribuições.

Seção III - Do Encarregado pelo Tratamento de Dados Pessoais

Art. 19. Compete ao Encarregado pelo Tratamento de Dados Pessoais:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da Autoridade Nacional de Proteção de Dados - ANPD e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares;

V - requerer relatório das áreas responsáveis por tratamento de dados pessoais no âmbito dos órgãos administrativos contendo, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados; e

VI - atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), na forma da Lei nº 13.709/2018 .

CAPÍTULO V - DAS DISPOSIÇÕES FINAIS

Art. 20. O órgão de Direção Geral do SETIC poderá expedir regulamentos complementares necessários à aplicação desta Instrução Normativa.

Art. 21. Os órgãos e entidades do Poder Executivo do Estado do Rio de Janeiro deverão cumprir o previsto no art. 9º no prazo de 120 (cento e vinte) dias a contar da data de publicação desta Instrução Normativa.

Parágrafo único. O Anexo Único desta Instrução Normativa deverá permanecer disponível no Portal do SETIC.

Art. 22. Esta Instrução Normativa entra em vigor na data de sua publicação.

Rio de Janeiro, 28 de abril de 2022

JOSÉ MAURO DE FARIAS JUNIOR

Presidente