Governo do Estado do Rio de Janeiro
Secretaria de Estado de Polícia Militar

PORTARIA SEPM SEI N.º 1065 DE 19 DE FEVEREIRO DE 2024

INSTITUI AS POLÍTICAS RELATIVAS À SEGURANÇA DA INFORMAÇÃO EM SOLUÇÕES DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO EM ÂMBITO DA SECRETARIA DE ESTADO DE POLÍCIA MILITAR, E DÁ OUTRAS PROVIDÊNCIAS.

O SECRETÁRIO DE ESTADO DE POLÍCIA MILITAR, no uso de suas atribuições legais,

CONSIDERANDO:

– o que consta no processo nº SEI-350011/000101/2024;
– o disposto na Instrução Normativa PRODERJ/PRE Nº 2 de 28 de abril de 2022;
– 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 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 da Polícia
Militar do Estado do Rio de Janeiro;
– a promoção do aperfeiçoamento das boas práticas da área de segurança da informação, estimular e fortalecer essa
cultura na Secretaria de Estado de Polícia Militar;
– 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 estabelecidas as políticas relativas à Segurança da Informação em soluções de Tecnologia da Informação e Comunicação, em âmbito da Secretaria de Estado de Polícia Militar – SEPM do Estado do Rio de Janeiro, na forma das disposições desta Portaria, com a finalidade de aprimorar a segurança da informação no âmbito da Administração Pública Estadual.

Parágrafo Único. Para os fins do disposto neste instrumento normativo, 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.

CAPÍTULO II – DOS PRINCÍPIOS

Art. 2º As ações de segurança da informação e comunicação previstas neste instrumento normativo 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 Federativa do Brasil, 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 da Polícia Militar do Estado do Rio de Janeiro, 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 militares, servidores, terceiros e fornecedores, em qualquer vínculo, função ou nível hierárquico na Polícia Militar do Estado do Rio de Janeiro, 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 ser instalados nas unidades da instituição mecanismos de proteção que impeçam acesso indevido aos ativos tecnológicos, bem como às áreas em que estes se encontram.

Art. 6º Toda informação custodiada em ativos tecnológicos 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 a instituição adotar através da Diretoria Geral de Tecnologia da Informação e Comunicação – DGTIC, na forma do art. 9º deste instrumento normativo.

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 tecnológicos da instituição.

Art. 9º As repartições da instituição, quer administrativas, quer operacionais, deverão manter procedimentos de segurança da informação com base nas diretrizes estabelecidas neste instrumento normativo, bem como nos da DGTIC, para orientar a correta utilização dos recursos computacionais em suas redes.

Seção II – Das Diretrizes Específicas

Art. 10. A DGTIC, ao estabelecer os procedimentos de segurança da informação, previstos no art. 9º, deverá 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 em âmbito da Polícia Militar;
II – Referências legais e normativas: identificar as referências legais e normativas utilizadas para a elaboração dos 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. 14;
b) Responsável pelo Tratamento e Resposta a Incidentes, na forma do art. 15;
c) Encarregado pelo Tratamento de Dados Pessoais, na forma do art. 16.
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 Fica designada a Diretoria de Sistemas de Informação – DSI, como o titular da gestão de segurança da informação em âmbito da SEPM, cabendo a esta Diretoria a responsabilidade pelo Tratamento e Resposta a Incidentes, com as respectivas competências, nos termos dos art. 14 e 15 da Instrução Normativa PRODERJ/PRE nº 2 de 28 de abril de 2022.

Art. 11. Quaisquer pessoas que tenham contato com os recursos de tecnologia da informação e comunicação em âmbito da SEPM, 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 disposto no anexo I da Resolução SEPM Nº 5.146 de 30 de janeiro de 2024, a qual institui a Política de Dados e Privacidade em âmbito da SEPM.

Art. 12. Os contratos com terceiros deverão estabelecer cláusulas de segurança da informação, de forma a resguardar o sigilo e a confidencialidade de toda e qualquer informação constante nos ativos tecnológicos geridos pela instituição.

Seção III – Das Normas Complementares

Art. 13. Com o propósito de assegurar a confidencialidade, disponibilidade e integridade dos ativos tecnológicos, a DGTIC instituirá normas complementares a este instrumento normativo, a serem observadas por todas as repartições das unidades da SEPM, para regular os aspectos pontuais de segurança da informação.
Parágrafo único. As normas complementares deverão permanecer disponíveis no site da SEPM.

CAPÍTULO IV – DOS AGENTES NOS ÓRGÃOS E ENTIDADES

Seção I – Do Gestor de Segurança da Informação

Art. 14. Compete ao Gestor de Segurança da Informação:
I – elaborar e atualizar periodicamente os procedimentos de segurança da informação da SEPM 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 da SEPM;

III – promover a cultura de segurança da informação no âmbito da SEPM;
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; e
VI – propor recursos necessários às ações de segurança da informação, no âmbito de atuação da SEPM;

Parágrafo único. O Gestor de Segurança da Informação será designado dentre os servidores públicos ocupantes de cargos efetivos lotados na DGTIC, com capacitação técnica compatível às suas atribuições.

Seção II – Do Responsável pelo Tratamento e Resposta a Incidentes

Art. 15. 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, na forma do art. 5º, VIII da LGPD 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 capacitação técnica compatível às suas atribuições.

Seção III – Do Encarregado pelo Tratamento de Dados Pessoais

Art. 16. 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, na forma do art. 5º, VI da LGPD, 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. 17. A DGTIC poderá expedir normas complementares necessários à aplicação deste instrumento normativo.

Art. 18. Fica estabelecido o prazo não superior a 120 (cento e vinte) dias, a contar da data da publicação deste instrumento normativo para o cumprimento do previsto no art. 9º.

Art. 19. Este instrumento normativo entra em vigor na data de sua publicação.

Rio de Janeiro, 19 de Fevereiro de 2024.

LUIZ HENRIQUE MARINHO PIRES
Secretário de Estado de Polícia Militar