Protocolo: 945603
Data: 11/12/2023
Título: DECRETO RIO Nº 53700
Página(s): a

DECRETO RIO Nº 53700 DE 8 DE DEZEMBRO DE 2023

Institui a Política de Segurança da Informação - PSI no âmbito do Poder Executivo Municipal, e dá outras providências.

O **PREFEITO DA CIDADE DO RIO DE JANEIRO** no uso das atribuições que lhe são conferidas pela legislação em vigor e

CONSIDERANDO que a manutenção de níveis adequados de segurança das informações tratadas pela Administração Pública Municipal é requisito imprescindível à consolidação de sua credibilidade junto ao cidadão;

CONSIDERANDO ser crucial a manutenção da integridade, disponibilidade, confidencialidade e autenticidade das informações tratadas pelos órgãos e entidades municipais visando garantir a confiabilidade de seus processos e serviços;

CONSIDERANDO que as informações são armazenadas em diferentes formas, veiculadas em diferentes meios, sejam físicos ou digitais, sendo, portanto vulneráveis a incidentes como desastres naturais, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto;

CONSIDERANDO a necessidade de aprimoramento contínuo das ações de governança e gestão de Segurança da Informação visando à sua compatibilização aos cenários de risco cibernético continuamente em evolução,

DECRETA:

Art. 1º Este Decreto institui a Política de Segurança da Informação - PSI no âmbito do Poder Executivo Municipal.

Parágrafo único. Todos os instrumentos normativos gerados a partir da Política de Segurança da Informação - PSI são partes integrantes desta e emanam dos princípios e diretrizes nela estabelecidos.

Art. 2º Esta política e suas normas complementares aplicam-se a toda Administração Pública Municipal, seus agentes públicos, independentemente de sua função, cargo, ou vínculo empregatício, aos prestadores de serviços, estagiários e pessoas físicas ou jurídicas que estejam autorizadas a tratar as informações municipais em quaisquer meios.

Parágrafo único. Os prestadores de serviços e as pessoas físicas e jurídicas em geral, que se vincularam à Administração por meio de instrumento de natureza contratual ou convenial em data anterior à vigência deste Decreto, apenas obedecerão aos seus termos por meio de previsão expressa em eventual termo aditivo ou prorrogação de ajuste.

Art. 3º Todos os processos de contratação de produtos e serviços, convênios, acordos e outros instrumentos congêneres celebrados pela Administração Pública Municipal devem ser analisados quanto aos aspectos relacionados à Segurança da Informação de forma que estejam sujeitos a

requisitos de conformidade a esta Política e às suas normas complementares.

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS
Seção I
Dos Objetivos

Art. 4º A Política de Segurança da Informação tem os seguintes objetivos:

I - definir princípios, diretrizes, responsabilidades e competências relacionadas à Governança e Gestão de Segurança da Informação;

II - conduzir os órgãos e entidades municipais a níveis de risco gerenciáveis no que diz respeito à Segurança da Informação;

III - resguardar a disponibilidade, integridade, confidencialidade e autenticidade das informações que suportam as atividades e os objetivos estratégicos dos órgãos e entidades municipais;

IV - fomentar o comprometimento dos agentes públicos na implantação e melhoria contínua de uma cultura de Segurança da Informação nos órgãos e entidades municipais.

Seção II
Dos Princípios Básicos

Art. 5º As ações de Segurança da Informação devem observar os seguintes princípios:

I - publicidade: garantir a divulgação de todas as medidas de gestão de riscos de Segurança da Informação, observando os critérios legais de sigilo aplicáveis;

II - proporcionalidade: ser proporcionais ao valor da informação e ao nível de risco ao qual estiverem expostas;

III - completude: cobrir todo o ciclo de vida da informação levando em conta todos os ativos que a suportam, sejam eles físicos, tecnológicos ou humanos;

IV - privacidade: assegurar o direito individual e coletivo das pessoas à inviolabilidade da sua intimidade e ao sigilo de seus dados pessoais, nos termos previstos na legislação vigente.

CAPÍTULO II
DOS TERMOS E DEFINIÇÕES

Art. 6º Para fins desta Política, considera-se:

I - acesso: capacidade de usar um ativo da informação (por exemplo: ler, criar, modificar ou excluir um arquivo; executar um programa; se conectar a um dispositivo, a uma rede, a um sistema, a um serviço ou entrar em áreas de acesso restrito que hospedam informações sensíveis);

II - ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos seus ativos ou prejuízos decorrentes de situações inesperadas (por exemplo: incêndio, falha de equipamentos, indisponibilidade de sistemas ou serviços, destruição de informações sensíveis, dentre outros);

III - ativo da informação: informação, processo ou ativo físico, tecnológico ou humano que suporta as operações de coleta, armazenamento, processamento, compartilhamento ou descarte de informações;

IV - ativo tecnológico: equipamento de TIC, software ou aplicação que suporta as atividades, processos de negócio e serviços de uma organização;

V - autenticidade: garantia de que os ativos da informação identificados em um processo de comunicação como remetentes ou destinatários sejam realmente quem dizem ser, ou seja, diz

respeito à veracidade das identidades dos ativos envolvidos em um processo de comunicação;

VI - classificação da informação: refere-se ao grau de sensibilidade de uma informação diante de uma possível quebra de segurança, ou seja, do comprometimento dos princípios básicos de Segurança da Informação, quais sejam confidencialidade, integridade e disponibilidade.

VII - confidencialidade: propriedade que garante que a informação só esteja disponível a indivíduos ou processos autorizados;

VIII - continuidade de negócios: capacidade estratégica e tática dos órgãos ou entidades do Município de se planejar e responder a incidentes que gerem interrupções em suas atividades ou serviços, visando minimizar impactos e manter suas operações em um nível aceitável de disponibilidade previamente definido;

IX - custodiante: pessoa física ou jurídica que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de informações que não lhe pertencem, mas que estão sob sua custódia;

X - disponibilidade: propriedade que garante que a informação só esteja disponível às pessoas e aos processos autorizados a qualquer momento em que sejam requeridas;

XI - equipamento ou equipamento de TIC: componente da infraestrutura de Tecnologia da Informação e Comunicação (TIC) (por exemplo: computador, notebooks, tablets, smartphones, servidores, roteadores, switches, etc);

XII - grupo de Prevenção, Tratamento e Resposta a Incidentes: agentes responsáveis por receber, analisar e responder às notificações e atividades relacionadas a incidentes de Segurança da Informação;

XIII - integridade: propriedade que garante que a informação está intacta e protegida contra perda, dano ou modificação não autorizada;

XIV - plano de gerenciamento de incidentes: plano de ação claramente definido e documentado para ser usado quando ocorrer um incidente;

XV - risco: probabilidade de ameaças explorarem vulnerabilidades, comprometendo a confidencialidade, integridade ou disponibilidade da informação, causando impactos para as atividades da Administração Pública Municipal;

XVI - sistema de informação: sistema composto por um conjunto de ativos da informação que tem por objetivo armazenar, transportar e processar informações visando suportar funções, serviços ou processos da Administração Pública Municipal;

XVII - usuário: qualquer pessoa autorizada a ler, inserir ou atualizar informações em um sistema de informação;

XVIII - vulnerabilidade: fragilidade presente ou associada a ativos da informação que, ao ser explorada por ameaças, permite a ocorrência de um incidente de segurança comprometendo um ou mais princípios de segurança da informação (confidencialidade, integridade e disponibilidade).

CAPÍTULO III
DAS COMPETÊNCIAS E RESPONSABILIDADES
Seção I
Das Competências

Art. 7º Compete à Secretaria Municipal da Casa Civil - CVL:

I - consolidar e coordenar as ações de gestão de riscos em Segurança da Informação no âmbito da

Administração Pública Municipal;

II - deliberar, analisar e revisar as normas complementares à Política de Segurança da Informação;

III - definir as metodologias referentes à gestão de riscos em Segurança da Informação;

IV - promover a divulgação das políticas, normas e melhores práticas de gestão de riscos no tema de Segurança da Informação para todos os órgãos e entidades municipais;

V - definir as estratégias para a implementação desta Política e de suas normas complementares;

VI - receber, analisar e consolidar os resultados relativos às auditorias de nível de conformidade dos órgãos e entidades municipais às políticas e normas de Segurança da Informação;

VII - atualizar periodicamente, mediante ato regulamentar, a Política de Segurança da Informação.

Art. 8º Compete à Empresa Municipal de Informática - IPLANRIO, em seu âmbito de atuação:

I - instituir e coordenar o Grupo de Prevenção, Tratamento e Resposta a Incidentes;

II - elaborar, implantar e gerenciar o programa de continuidade de negócios dos serviços corporativos;

III - planejar, coordenar, supervisionar e controlar as atividades de TIC visando garantir conformidade a esta Política e às suas normas complementares;

IV - prever orçamento específico para as ações de Segurança da Informação, no âmbito da PCRJ;

V - oferecer apoio operacional nas ações corretivas em casos de descumprimento da Política de Segurança da Informação ou de suas normas complementares, nos órgãos e entidades da PCRJ.

Parágrafo único. Compete ao Grupo de Prevenção, Tratamento e Resposta a Incidentes:

I - executar as atividades de prevenção, tratamento e resposta a incidentes de segurança por intermédio de processos em conformidade com as melhores práticas relacionadas à matéria;

II - elaborar o plano de gerenciamento de incidentes no Datacenter;

III - executar as atividades de recuperação dos sistemas e serviços comprometidos por incidentes de segurança de forma integrada com as respectivas equipes de administração dos ativos que os suportam.

Art. 9º Compete aos órgãos e entidades da Administração Pública Municipal, em seu âmbito de atuação:

I - implementar a Política de Segurança da Informação;

II - apoiar a elaboração da estratégia de gestão de riscos de segurança da informação;

III - implementar o programa de gestão de riscos de segurança da informação;

IV - disseminar esta Política e suas normas complementares;

V - aplicar as ações corretivas, com apoio operacional da IPLANRIO, e disciplinares nos casos de descumprimento da Política de Segurança da Informação ou de suas normas complementares.

Art. 10. Compete à Controladoria Geral do Município do Rio de Janeiro - CGM auditar periodicamente o cumprimento da Política de Segurança da Informação e de suas normas

complementares, analisando e avaliando a eficácia das suas medidas de implementação.

Seção II
Das Responsabilidades
Subseção I
Dos usuários

Art. 11. É de responsabilidade dos usuários dos ativos da informação:

I - gerenciar os ativos da informação sob sua responsabilidade e garantir que sejam utilizados exclusivamente para os fins previstos;

II - realizar suas competências funcionais em aderência a todas as políticas, normas e procedimentos de segurança da informação a elas relacionados;

III - comunicar prontamente ao seu chefe imediato, ou ao preposto em caso de prestadores de serviço, quaisquer desvios das políticas, normas e procedimentos estabelecidos, ou incidentes de segurança que tenha conhecimento;

IV - tratar a informação de acordo com a sua classificação, adotando as medidas de proteção previstas para o tratamento dos riscos a que estão sujeitos os ativos de informação sob sua custódia;

V - manter-se atualizado quanto a esta Política e normas complementares.

Subseção II
Dos Custodiantes

Art. 12. Ao custodiante da informação cabem as seguintes responsabilidades:

I - zelar pela disponibilidade, integridade e confidencialidade das informações sob sua custódia;

II - utilizar os ativos da informação sob sua custódia exclusivamente para os fins previstos;

III - comunicar prontamente ao seu chefe imediato, ou ao preposto em caso de prestadores de serviço, quaisquer desvios das políticas, normas e procedimentos estabelecidos, ou incidentes de segurança que tenha conhecimento;

IV - preservar a classificação dos ativos da informação aos quais tiver acesso em decorrência do exercício de suas funções, adotando as medidas de proteção previstas para o tratamento dos riscos a que estejam sujeitos.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 13. A Política de Segurança da Informação - PSI - será regulamentada por atos da Secretaria Municipal da Casa Civil, no prazo de até 180 (cento e oitenta) dias da publicação deste Decreto.

Parágrafo único. Os atos regulamentares editados pela Secretaria Municipal da Casa Civil deverão ser revisados com periodicidade máxima de 2 (dois) anos a contar da data de sua publicação.

Art. 14. As ações que violem esta Política ou suas normas complementares são passíveis de sanções administrativas, conforme a legislação em vigor.

Art. 15. Este Decreto entra em vigor na data de sua publicação.

Art. 16. Ficam revogados o Decreto Rio nº 44.276, de 01 de março de 2018, a Deliberação nº 01, de 28 e março de 2018, o inciso IV, do art. 5º do Decreto Rio nº 49.558, de 6 de outubro de 2021 e

demais disposições em contrário.

Rio de Janeiro, 8 de dezembro de 2023; 459º ano da fundação da Cidade.

EDUARDO PAES