DECRETO Nº 491, DE 09 DE JULHO DE 2026

Número completo	Decreto nº 491/2026
Tipo	Decreto
Data de publicação	09/07/2026
Status	VIGENTE
Link DOM/JOM	https://www.marica.rj.gov.br/dom/ed-077/

EMENTA

INSTITUI A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DO PODER EXECUTIVO MUNICIPAL.

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;

CONSIDERANDO as diretrizes estabelecidas no Decreto Municipal nº 840, de 05 de abril de 2022, que regulamenta a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) no âmbito do Município de Maricá, e a necessidade de mútua complementariedade entre as ações de segurança cibernética e a proteção de dados pessoais.

O **PREFEITO MUNICIPAL DE MARICA,** no uso de suas atribuições legais;

DECRETA:

Capítulo I

DISPOSIÇÕES INICIAIS

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 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, deverão adequar-se aos seus termos regulamentares no prazo de até 180 (cento e oitenta) dias a contar de sua publicação, mediante notificação formal ou repactuação de metas de conformidade.

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 II

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 apropriados;

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, em estrita observância aos ditames da Lei Federal nº 13.709/2018 – LGPD e do Decreto Municipal nº 840/2022.

Capítulo III

DOS TERMOS E DEFINIÇÕES

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

I – acesso: capacidade de usar um ativo da informação, como 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, como 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 os 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 comprometimento dos princípios básicos de Segurança da Informação;

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 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, como 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.

Capítulo IV
DAS COMPETÊNCIAS E RESPONSABILIDADES

SEÇÃO I
Das Competências

Art. 7º Compete ao Órgão Responsável pela Gestão de Tecnologia da Prefeitura:

I – consolidar e coordenar as ações de gestão de riscos em Segurança da Informação no âmbito da Administração Pública Municipal;

II – deliberar, analisar, revisar e publicar as normas complementares necessárias para suplementar e detalhar as diretrizes desta 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;

VIII – homologar os planos técnicos de gerenciamento de incidentes e de continuidade de negócios propostos pelas entidades executoras de TIC do município.

Art. 8º Compete à CODEMAR através de sua Diretoria de Tecnologia, em seu âmbito de atuação técnico-operacional:

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 sob sua custódia;

III – executar, gerenciar e prover suporte técnico às atividades de TIC, garantindo a conformidade operacional dos ativos sob sua gestão a esta Política e às suas normas complementares;

IV – submeter ao Órgão Responsável pela Gestão de Tecnologia da Prefeitura a previsão orçamentária das necessidades tecnológicas de Segurança da Informação para a infraestrutura pública administrada;

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 Municipalidade.

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. Sempre que um incidente de segurança da informação gerenciado sob as diretrizes desta PSI envolver indícios ou confirmação de vazamento de dados pessoais de cidadãos ou servidores, o Grupo de Resposta a Incidentes notificará imediatamente o Encarregado Geral da Proteção de Dados e a Comissão Permanente Municipal de Proteção de Dados – CPMPD, instituída pelo Decreto Municipal nº 840/2022 e nomeada pela Portaria SEGG nº 002/2025.

Parágrafo único. A atuação técnica da CODEMAR nos incidentes cibernéticos restringe-se ao suporte tecnológico e à mitigação de riscos à infraestrutura, cabendo à CPMPD e ao Encarregado Geral as deliberações sobre o impacto administrativo e regulatório perante a Autoridade Nacional de Proteção de Dados – ANPD.

Art. 10. 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 Diretoria de Tecnologia da CODEMAR, e disciplinares nos casos de descumprimento da Política de Segurança da Informação ou de suas normas complementares.

Art. 11. Compete à Controladoria Geral do Município de Maricá – 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. 12. 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, sem prejuízo do cumprimento das salvaguardas e rotinas de privacidade determinadas pelo Decreto Municipal nº 840/2022;

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

Subseção II

Dos Custodiantes

Art. 13. 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 V

DO COMITÊ MULTIDISCIPLINAR DE SEGURANÇA DA INFORMAÇÃO – CMSI

SEÇÃO I

Disposições Iniciais

Art. 14. Fica instituído o **Comitê Multidisciplinar de Segurança da Informação – CMSI**, órgão colegiado de natureza consultiva e deliberativa, responsável pela governança estratégica de segurança cibernética no município.

SEÇÃO II

Da Composição e Diretrizes

Art. 15. O CMSI atuará em estrita consonância com os princípios da Política de Segurança da Informação – PSI e com as salvaguardas de privacidade estabelecidas no Decreto Municipal nº 840/2022 – LGPD.

Art. 16. O Comitê será composto por membros titulares e suplentes indicados pelas seguintes pastas:

I – órgão responsável pela Gestão de Tecnologia da Prefeitura, que exercerá a Presidência do Comitê;

II – Controladoria Geral do Município – CGM;

III – Procuradoria Geral do Município – PGM;

IV – Diretoria de Tecnologia da Companhia de Desenvolvimento de Maricá – CODEMAR.

Parágrafo único. A participação no CGSI será considerada prestação de serviço público relevante, não sendo remunerada.

SEÇÃO III

Das Regras de Funcionamento e Prazos

Art. 17. Compete ao Comitê:

I – analisar, deliberar e homologar propostas de novas Normas Complementares à PSI antes de sua publicação;

II – validar e aprovar os planos técnicos de gerenciamento de incidentes e de continuidade de negócios;

III – reunir-se de forma ordinária a cada bimestre, ou extraordinariamente por convocação de seu Presidente.

Art. 18. Os titulares das pastas indicadas no art. 16 deverão nomear seus respectivos representantes no prazo improrrogável de até 15 (quinze) dias a contar da data da publicação deste Decreto.

Art. 19. Todas as reuniões do Comitê deverão, obrigatoriamente, ser lavradas em atas circunstanciadas, devidamente registradas e assinadas pelos membros presentes em livro próprio ou sistema eletrônico oficial, servindo como documento de evidência para auditorias da Controladoria Geral do Município e do TCE-RJ.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 20. A Política de Segurança da Informação será regulamentada e detalhada por meio de Normas Complementares – NC específicas editadas pelo Órgão Responsável pela Gestão de Tecnologia da Prefeitura, no prazo de até 180 (cento e oitenta) dias da publicação deste Decreto.

§ 1º As Normas Complementares disciplinarão, obrigatoriamente, os seguintes temas essenciais à suplementação desta PSI, sem prejuízo da edição de novas normas a qualquer momento, sempre que constatada a necessidade institucional ou a evolução dos cenários de risco:

I – gestão de fornecedores e operadores;

II – uso de recursos tecnológicos da prefeitura e diretrizes de BYOD;

III – gestão de identidade e controle de acessos;

IV – padrões técnicos e complexidade de senhas;

V – classificação da Informação, em estrita associação aos parâmetros da Lei de Acesso à Informação – LAI;

VI – Política de Mesa Limpa e Tela Limpa.

§ 2º Os atos regulamentares e as Normas Complementares editadas deverão ser revisados com periodicidade máxima de 2 (dois) anos a contar da data de sua publicação.

Art. 21. Fica estabelecido o prazo de transição de até 180 (cento e oitenta) dias, a contar da data de publicação das respectivas Normas Complementares, para que os órgãos e sistemas legados do Poder Executivo Municipal se adéquem integralmente às novas exigências operacionais.

Art. 22. As ações que violem a Política tratada neste Decreto ou suas normas complementares são passíveis de sanções administrativas e disciplinares, conforme a legislação estatutária e contratual em vigor.

Art. 23. Este Decreto entra em vigor na data de sua publicação.

REGISTRE-SE, PUBLIQUE-SE, CUMPRA-SE.

Gabinete do Prefeito, aos 9 dias do mês de julho de 2026.

Washington Luiz Cardoso Siqueira

PREFEITO DO MUNICÍPIO DE MARICÁ