



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

www.reginopolis.sp.gov.br | www.imprensaoficialmunicipal.com.br/reginopolis

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 1 de 35

SUMÁRIO

Poder Executivo	2
Atos Oficiais	2
Decretos	2
Outros atos oficiais	34
Licitações e Contratos	35
Aditivos / Aditamentos / Supressões	35
Ratificação	35

EXPEDIENTE

O Diário Oficial do Município de Reginópolis, veiculado exclusivamente na forma eletrônica, é uma publicação das entidades da Administração Direta e Indireta deste Município, sendo referidas entidades inteiramente responsáveis pelo conteúdo aqui publicado.

ACERVO

As edições do Diário Oficial Eletrônico de Reginópolis poderão ser consultadas através da internet, por meio do seguinte endereço eletrônico: www.reginopolis.sp.gov.br. Para pesquisa por qualquer termo e utilização de filtros, acesse www.imprensaoficialmunicipal.com.br/reginopolis. As consultas e pesquisas são de acesso gratuito e independente de qualquer cadastro.

ENTIDADES

Prefeitura Municipal de Reginópolis

CNPJ 44.556.033/0001-98
Rua Abraão Ramos, 327
Telefone: (14) 3589-9200 | (14) 3589-9201
Site: www.reginopolis.sp.gov.br
Diário: www.imprensaoficialmunicipal.com.br/reginopolis

Câmara Municipal de Reginópolis

CNPJ 51.499.085/0001-35
Rua Major Álvaro Fernandes de Freitas, 379
Telefone: (14) 3589-1288
Site: www.camarareginopolis.sp.gov.br



Diário Oficial Assinado Eletronicamente com Certificado Padrão ICPBrasil, em conformidade com a MP nº 2.200-2, de 2001

O Município de Reginópolis garante a autenticidade deste documento, desde que visualizado através do site www.reginopolis.sp.gov.br

Compilado e também disponível em www.imprensaoficialmunicipal.com.br/reginopolis



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 2 de 35

PODER EXECUTIVO

Atos Oficiais

Decretos

Decreto nº. 060, de 17 de novembro de 2.025.

"DISPÕE SOBRE PROCEDIMENTOS A SEREM OBSERVADOS E ADOTADOS NA ADMINISTRAÇÃO MUNICIPAL PARA O ENCERRAMENTO DO EXERCÍCIO de 2025, E DÁ OUTRAS PROVIDÊNCIAS".

JEFFERSON AUGUSTO RODRIGUES BUAVA, Prefeito Interino de Reginópolis, Comarca de Pirajuí, Estado de São Paulo, usando das atribuições que lhe confere o inciso I, do artigo 85, da Lei Orgânica do Município,

DECRETA:

Art. 1º - As Secretarias Municipais deverão realizar estudo prévio e planejar suas aquisições de bens e insumos necessários à sua manutenção.

Art. 2º - As despesas de vinculação legal ou contratual referente a Convênios e Programas, poderão ocorrer desde que haja disponibilidade financeira.

Art. 3º - Só serão autorizadas aquisições e contratações não essenciais às manutenções se devidamente justificadas e autorizadas pelo Sr. Prefeito Municipal.

Art. 4º - As notas de empenho do exercício de 2025 serão emitidas até o dia 10 de dezembro de 2025, ressalvados os casos abaixo discriminados:

I - Quando se tratar de despesas com pessoal, encargos com amortizações de dívida interna ou obrigações patronais;

II - Despesas com água, luz, telefone e outras despesas pertinentes ao funcionamento das atividades essenciais de saúde, educação, assistência social e infraestrutura básica de caráter urgente e necessário;

III - procedimentos licitatórios em andamento.

Parágrafo Único: A liquidação das despesas de que trata o "caput" deste artigo, deverá ocorrer até o dia 15/12/2025.

Art. 5º - Os pagamentos de despesas do exercício e de restos a pagar somente serão realizados até o dia 15/12/2025, com exceção às despesas relativas à pessoal, encargos sociais, amortização da dívida, despesas com água, luz, telefone, correio, ressalvados os casos em que haver disponibilidade financeira.

Art. 6º - Compete as Secretarias Municipais a responsabilidade no cumprimento deste Decreto e demais normas orçamentárias e financeiras.

Art. 7º - As medidas de que trata este Decreto, terá duração até a data de 31 de dezembro de 2025.

Art. 8º - Este Decreto entra em vigor na data de sua

publicação, revogadas as disposições em contrário.

Publique-se, registre-se e cumpra-se.

Reginópolis, 17 de novembro de 2025.

JEFFERSON AUGUSTO RODRIGUES BUAVA
Prefeito Interino

Registrado na secretária e publicado na forma da Lei vigente

DECRETO Nº. 061, DE 18 DE NOVEMBRO DE 2025.

"Revoga os Decretos nº 40/2024 e Portaria nº120/2025, e dá outras providências".

JEFFERSON AUGUSTO RODRIGUES BUAVA, Prefeito Interino de Reginópolis, Comarca de Pirajuí, Estado de São Paulo, usando das atribuições que lhe conferem a alínea "a", inciso I, do artigo 85, da Lei Orgânica do Município,

DECRETA:

Art. 1º Ficam revogados o Decreto nº 40/2024 e a Portaria nº120/2025, que tratam da instituição do Sistema Eletrônico de Informações do Estado de São Paulo - SEI/CIDADES como meio eletrônico para a formalização de processo administrativo no âmbito da Administração Direta e Indireta do Município de Reginópolis.

Art. 2. Este Decreto entrará em vigor na data de sua publicação.

Prefeitura do Município de Reginópolis, 18 de novembro de 2025.

JEFFERSON AUGUSTO RODRIGUES BUAVA
Prefeito Municipal

DECRETO Nº. 062, DE 18 DE NOVEMBRO DE 2025.

"Regulamenta a Lei Geral de Proteção de Dados e dá outras providências".

JEFFERSON AUGUSTO RODRIGUES BUAVA, Prefeito Interino de Reginópolis, Comarca de Pirajuí, Estado de São Paulo, usando das atribuições que lhe conferem a alínea "a", inciso I, do artigo 85, da Lei Orgânica do Município,

DECRETA:

REGULAMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º - Este Decreto regulamenta a [Lei Federal nº 13.709, de 14 de agosto de 2018](#), Lei de Proteção de Dados Pessoais (LGPD), no âmbito do Poder Executivo Municipal, estabelecendo competências, procedimentos e providências correlatas a serem observados por seus órgãos e entidades, visando garantir a proteção de dados pessoais.

Art. 2º - Para os fins deste decreto, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 3 de 35

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoal natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa indicada pelo controlador e operador como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

IX - agentes de tratamento: o controlador e o operador;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular dos dados concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - plano de adequação: conjunto das regras de boas práticas e de governança de dados pessoais que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos agentes envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos, o plano de respostas a incidentes de segurança e outros aspectos relacionados ao tratamento de dados pessoais;

XIV - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos

fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

XV - Autoridade Nacional de Proteção de Dados (ANPD): órgão da Administração Pública Federal responsável por zelar, implementar e fiscalizar o cumprimento desta lei em todo o território nacional.

Art. 3º - As atividades de tratamento de dados pessoais pelos órgãos e entidades municipais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comerciais e industriais;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de dados em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

CAPÍTULO - II

DAS RESPONSABILIDADES

SEÇÃO I

DAS RESPONSABILIDADES NA ADMINISTRAÇÃO PÚBLICA MUNICIPAL

Art. 4º O Poder Executivo Municipal, por meio de seus



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 4 de 35

Departamentos, nos termos da [Lei Federal nº 13.709, de 2018](#), deve realizar e manter continuamente atualizados:

I - o mapeamento dos dados pessoais existentes e dos fluxos de dados pessoais em suas unidades;

II - a análise de risco;

III - o plano de adequação, observadas as exigências do art. 11 deste decreto;

IV - o relatório de impacto à proteção de dados pessoais, quando solicitado.

Parágrafo único. Para fins do inciso III, do “caput” deste artigo, os Departamentos devem observar as diretrizes editadas pelo Controlador do Município e o Encarregado de Proteção de Dados do Município, após deliberação favorável da Comitê Municipal de Tecnologia da Informação (CMTI).

Art. 5º Fica designado o Encarregado de Proteção de Dados do Município como o Encarregado de Proteção de Dados Pessoais, para os fins do art. 41, da [Lei Federal nº 13.709, de 2018](#), que será nomeado por portaria.

Parágrafo único. A identidade e as informações de contato do encarregado devem ser divulgadas publicamente, de forma clara e objetiva, no Portal da Transparência, em seção específica sobre tratamento de dados pessoais.

Art. 6º Compete ao Encarregado de Proteção de Dados do Município, além das atribuições ordinárias para o desempenho das funções previstas na Lei 13.709, de 2018 e demais dispositivos deste decreto:

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

II - atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), cumprindo com atribuições que possam vir a ser estabelecidas pela ANPD;

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

IV - elaborar o Relatório de Impacto à proteção de dados pessoais com a descrição dos processos de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como, as medidas e salvaguardas e mecanismos de mitigação de riscos;

V - decidir sobre as sugestões formuladas pela autoridade nacional a respeito da adoção de padrões e de boas práticas para o tratamento de dados pessoais e providenciar a publicação dos relatórios de impacto à proteção de dados pessoais previstos nos termos do art. 32 da [Lei Federal nº 13.709, de 2018](#);

VII - executar as demais atribuições determinadas pelo controlador ou estabelecida em normas complementares.

VIII - submeter à Comitê Municipal de Tecnologia da Informação (CMTI), sempre que julgar necessário, matérias atinentes a este decreto;

CAPÍTULO III

DO TRATAMENTO DE DADOS PESSOAIS PELA

ADMINISTRAÇÃO PÚBLICA MUNICIPAL

Art. 7º. O tratamento de dados pessoais pelos órgãos e entidades da Administração Pública Municipal deve:

I - objetivar o exercício de suas competências legais ou o cumprimento das atribuições legais do serviço público, para o atendimento de sua finalidade pública e a persecução do interesse público;

II - observar o dever de conferir publicidade às hipóteses de sua realização, com o fornecimento de informações claras e atualizadas sobre a previsão legal, finalidade, os procedimentos e as práticas utilizadas para a sua execução.

Art. 8º. Os órgãos e as entidades da Administração Pública Municipal podem efetuar o uso compartilhado de dados pessoais com outros órgãos e entidades públicas para atender a finalidades específicas de execução de políticas públicas, no âmbito de suas atribuições legais, respeitados os princípios de proteção de dados pessoais elencados no art. 6º da Lei Federal nº 13.709, de 2018.

Art. 9º. É vedado aos órgãos e entidades da Administração Pública Municipal transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei Federal nº 12.527, de 2011;

II - nos casos em que os dados forem acessíveis publicamente, observadas as disposições da Lei Federal nº 13.709, de 2018;

III - quando houver previsão legal ou a transferência for respaldada, por meio de cláusula específica, em contratos, convênios ou instrumentos congêneres, cuja celebração deverá ser informada pelo responsável ao Encarregado de Proteção de Dados do Município para comunicação à autoridade nacional de proteção de dados;

IV - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

Parágrafo único. Em quaisquer das hipóteses previstas neste artigo:

I - a transferência de dados dependerá de autorização específica conferida pelo órgão municipal à entidade privada;

II - as entidades privadas deverão assegurar que não haverá comprometimento do nível de proteção dos dados garantido pelo órgão ou entidade municipal.

Art. 10. Os órgãos e entidades da Administração Pública Municipal podem efetuar a comunicação ou o uso compartilhado de dados pessoais a pessoa de direito privado, desde que:

I - o Encarregado de Proteção de Dados do Município informe a Autoridade Nacional de Proteção de Dados, na forma do regulamento federal correspondente;



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 5 de 35

II - seja obtido o consentimento do titular, salvo:

a) nas hipóteses de dispensa de consentimento previstas na Lei Federal nº 13.709, de 2018;

b) nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do art. 9, inciso II, deste decreto;

c) nas hipóteses do art. 11 deste decreto.

Parágrafo único. Sempre que necessário o consentimento, a comunicação dos dados pessoais a entidades privadas e o uso compartilhado entre estas e o órgãos e entidades municipais poderão ocorrer somente nos termos e para as finalidades indicadas no ato do consentimento.

Art. 11. Os planos de adequação devem observar, no mínimo, o seguinte:

I - publicidade das informações relativas ao tratamento de dados em veículos de fácil acesso, preferencialmente nas páginas dos órgãos e entidades na internet, bem como no Portal da Transparência, em seção específica a que se refere o parágrafo único do art. 5º deste decreto;

II - atendimento das exigências que vierem a ser estabelecidas pela Autoridade Nacional de Proteção de Dados, nos termos do art. 23, § 1º, e do art. 27, parágrafo único da Lei Federal nº 13.709, de 2018;

III - manutenção de dados em formato interoperável e estruturado para o uso compartilhado de dados com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Art. 12. Compete ao Comitê Municipal de Tecnologia da Informação (CMTI):

I - analisar e aprovar os procedimentos para a proteção e tratamento de dados no âmbito do Município de Reginópolis, elaborada e encaminhada pelo Encarregado de Proteção de Dados do Município;

II - atuar de forma deliberativa e consultiva quanto a qualquer assunto relacionado à LGPD, demais leis que possam colidir com o tema proteção de dados e sobre este decreto.

III - oferecer os subsídios técnicos necessários à edição das diretrizes pelo encarregado da proteção de dados, para a elaboração dos planos de adequação;

IV - orientar, sob o ponto de vista tecnológico, as Secretarias na implantação dos respectivos planos de adequação.

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

Art. 13. Os Departamentos deverão comprovar ao Encarregado de Proteção de Dados do Município estar em conformidade com o disposto no art. 4º deste decreto.

Art. 14. Este Decreto entrará em vigor na data de sua publicação.

Prefeitura do Município de Reginópolis, 18 de novembro de 2025.

JEFFERSON AUGUSTO RODRIGUES BUAVA

Prefeito Municipal

Registrado na Secretaria e publicado na forma da Lei.

.....



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 6 de 35

DECRETO Nº. 063, DE 18 DE NOVEMBRO DE 2025.

“Institui a Política de Segurança da Informação e dá outras providências”.

JEFFERSON AUGUSTO RODRIGUES BUAVA,

Prefeito Interino de Reginópolis, Comarca de Pirajuí, Estado de São Paulo, usando das atribuições que lhe conferem a alínea “a”, inciso I, do artigo 85, da Lei Orgânica do Município,

D E C R E T A:

Art. 1º Fica instituída a Política de Segurança da Informação (PSI), com a finalidade de definir princípios, normas e responsabilidades para a gestão segura das informações no âmbito da Administração Pública Municipal.

Art. 2º São objetivos da Política Municipal de Segurança da Informação:

- I – proteger as informações institucionais contra ameaças internas ou externas;
- II – assegurar a continuidade dos serviços públicos;
- III – promover o uso adequado dos recursos tecnológicos;
- IV – estabelecer responsabilidades e boas práticas de segurança;
- V – garantir conformidade com legislações vigentes, incluindo a Lei Geral de Proteção de Dados (LGPD).

Art. 3º Todos os servidores, colaboradores, estagiários e terceiros que utilizem recursos de informação do Município ficam sujeitos às disposições desta Política.

Art. 4º Compete aos titulares das Secretarias, Setores e demais unidades administrativas:

- I – assegurar a aplicação das normas desta Política em suas áreas;
- II – comunicar incidentes ou riscos identificados ao setor de Tecnologia da Informação.

Art. 5º Compete ao Setor de Tecnologia da Informação:

- I – manter e atualizar a Política de Segurança da Informação;
- II – garantir a implementação de controles e mecanismos de segurança;
- III – monitorar incidentes e promover ações preventivas e corretivas;
- IV – orientar e capacitar usuários sobre boas práticas de segurança.

Art. 6º A Política Municipal de Segurança da Informação, em anexo, passa a integrar este Decreto.

Art. 7. Este Decreto entrará em vigor na data de sua publicação.

Prefeitura do Município de Reginópolis, 18 de novembro de 2025.

JEFFERSON AUGUSTO RODRIGUES BUAVA
Prefeito Municipal

Registrado na Secretaria e publicado na forma da Lei vigente.



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 7 de 35



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 8 de 35

HISTÓRICO DE ALTERAÇÕES

Data	Revisão	Descrição	Autor
14/11/2025	0	Versão inicial	Marcos Dóta de Lima

PRINCIPAIS ATUALIZAÇÕES

Data	Revisão	Descrição	Autor
14/11/2025	0	Versão inicial	A elaboração desta PSI foi precedida por uma avaliação abrangente das necessidades, deficiências e riscos associados ao uso das tecnologias de informação e comunicação na administração pública.

Nota de versão

Esta é a primeira versão da Política de Segurança da Informação (PSI) da Prefeitura Municipal de Reginópolis, realizada para avaliar as necessidades, expectativas e riscos associados ao uso das tecnologias de informação e comunicação na administração pública municipal, garantindo que a política reflita com precisão a realidade do município. O objetivo é envolver todas as secretarias, departamentos e setores na concepção do documento, assegurando que as ações planejadas atendam às necessidades identificadas e mitiguem deficiências, promovendo uma gestão eficiente da tecnologia da informação e comunicação e garantindo a segurança dos dados. Esta versão considera as diretrizes da Lei Geral de Proteção de Dados (LGPD), do Marco Civil da Internet, das estratégias de governo digital e da nova lei de licitações, visando à melhoria contínua na proteção das informações sob a custódia do município.



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 9 de 35

Sumário

1. Referências legais e normativas	6
2. Siglas, termos e definições	6
3. Objetivos da Política de Segurança da Informação (PSI)	8
Objetivos Específicos:	8
4. Princípios	9
5. Diretrizes	9
Diretrizes Específicas:	9
6. Responsabilidades	10
6.1 Colaboradores	10
6.2 Gestores de Pessoas e/ou Processos	10
6.3 Setor de Recursos Humanos	10
6.4 Custodiantes da Informação (Área de Tecnologia da Informação)	10
7. Políticas	10
7.1 Controle de Acesso Lógico	10
7.1.1 Conta de Acesso	10
7.1.2 Princípio do Privilégio Mínimo	10
7.1.3 Acesso Remoto	10
7.1.4 Solicitação de Acesso	11
7.1.5 Senhas de Usuários	11
7.1.6 Recuperação de Senha	11
7.1.7 Comunicação de Anomalias	11
7.1.8 Contas Administrativas	11
7.2 Controle de Acesso à Infraestrutura	11
7.2.1 O acesso ao datacenter	11
7.2.3 A porta de acesso	11
7.3 Controle de Acesso à Internet	11
7.3.1 Uso Permitido	12
7.3.2 Uso Profissional	12
7.3.3 Monitoramento	12
7.3.4 Restrições de Acesso	12
7.3.5 Proibições Específicas	12
7.3.6 Uso do E-mail Corporativo	13



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 10 de 35

7.3.7 Responsabilidade pela Informação	13
7.3.8 Atividades Ilegais	13
7.3.9 Equipamentos Pessoais	13
7.3.10 Disponibilidade da Política	13
7.3.11 Dúvidas e Comentários.....	13
7.4 E-mail Corporativo	13
7.4.1 Uso do Domínio Corporativo.....	13
7.4.2 Atividades Ilegais	13
7.4.3 Ações Nocivas	13
7.4.4 Conteúdo Inapropriado	13
7.4.5 Anúncios e Mensagens Indesejadas	14
7.4.6 Envio de Arquivos	14
7.4.7 Divulgação de Contatos.....	14
7.4.8 Vulnerabilidade Legal	14
7.4.9 Informações Confidenciais	14
7.4.10 Atividades Lesivas	14
7.4.11 Responsabilidades do Usuário	14
7.5 Uso de Equipamentos de Informática	14
7.5.1 Uso Exclusivo	15
7.5.2 Identificação da Estação de Trabalho.....	15
7.5.3 Proibições de Gravação	15
7.5.4 Armazenamento de Dados	15
7.5.5 Cópia de Segurança	15
7.5.6 Reparo de Equipamentos	15
7.5.7 Equipamentos Pessoais.....	15
7.5.8 Comunicação de Danos.....	15
7.5.9 Furto ou Roubo	16
7.5.10 Adesivos e Modificações	16
7.5.11 Zelo pelo Equipamento.....	16
7.5.12 Verificação do Termo de Responsabilidade	16
7.5.13 Configurações do Equipamento	16
7.5.14 Uso Não Autorizado.....	16
7.5.15 Conexão à Rede	16



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 11 de 35

7.5.16 Antivírus Atualizado.....	16
7.5.17 Armazenamento Seguro	16
7.5.18 Acesso às Áreas Críticas	16
7.5.19 Uso Exclusivo dos Notebooks	16
7.5.20 Restrições no Uso do Notebook.....	17
7.5.21 Armazenamento Pessoal	17
7.5.22 Zelo pelos Equipamentos de Informática.....	17
7.5.23 Reposição por Mau Uso ou Perda.....	17
7.6 Backups.....	17
7.6.1 Automação dos Backups.....	17
7.6.2 Gestão de Sistemas de Backup	17
7.6.3 Monitoramento dos Backups	17
7.7 Auditoria, monitoramento e registro de logs de acesso	17
7.7.1 Implantação de Sistemas de Monitoramento.....	17
7.7.2 Divulgação de Informações	18
7.7.3 Inspeção Física.....	18
7.7.4 Sistemas de Proteção	18
7.7.5 Registro Automático de Credenciais	18
7.8 Política de Uso de Impressoras	18
7.8.1 Registro de Impressões.....	18
7.8.2 Uso Exclusivo para Fins Institucionais	18
7.8.3 Consciência Ecológica.....	18
7.8.4 Proibição de Impressão de Conteúdo Inadequado	18
7.8.5 Manutenção da Privacidade.....	19
7.8.6 Limitação de Acesso	19
7.8.7 Monitoramento e Auditoria	19
7.8.8 Responsabilidade pelo Equipamento	19
7.9 Uso de Assinaturas Digitais.....	19
7.9.1 Responsabilidade do Usuário.....	19
7.9.2 Comunicação de Incidentes.....	19
7.9.3 Revogação do Certificado.....	19
7.10 Utilização do Sistema de CFTV	20
7.11 Abertura de Chamados	20



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 12 de 35

8. Cumprimento	20
9. Considerações Finais	20
TERMO DE CIÊNCIA - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	6



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 13 de 35



PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Referências legais e normativas

ABNT NBR ISO/IEC 27001:2024 – Sistemas de gestão de segurança da informação.
ABNT NBR ISO/IEC 27000:2024
Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet.
Lei Geral de Proteção de Dados (LGPD) Lei 13.709/2018.

2. Siglas, termos e definições

Ação de evitar o risco - Decisão de não se envolver ou agir de forma a se retirar de uma situação de risco.

Aceitar/Reter o risco - Aceitação do ônus da perda ou do benefício do ganho associado a um determinado risco.

Ameaça - Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou uma organização.

Ativo - Qualquer elemento que tenha valor para a organização.

Ativos Críticos de Tecnologia da Informação - São os Ativos de Tecnologia da Informação indispensáveis aos processos diretamente relacionados aos objetivos estratégicos da Instituição.

Ativo de Informação - Dados, informações e conhecimentos obtidos, gerados, tratados e/ou armazenados, como por exemplos base de dados, arquivos, contratos, acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos e planos institucionais, processos de trabalho, entre outros.

Ativo de Tecnologia da Informação - Composto por ativos de *software* e ativos físicos, permitindo o armazenamento, a transmissão e processamento das informações. Exemplos de ativos de *software*: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários. Exemplos de ativos físicos: os equipamentos computacionais fixos e móveis, equipamentos utilizados na Política de Segurança da Informação e Comunicações para comunicação de dados e mídias removíveis.

Backup - Cópias de segurança de arquivos.

Certificado Digital - Identificação pessoal CPF/CNPJ de forma digital.

Conformidade - Estar de acordo com determinadas normas, regras ou preceitos.

Contas de Serviço - Contas de acesso à rede corporativa de computadores necessários a um procedimento automático (aplicação, *script* etc.), sem qualquer intervenção humana no seu uso.



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 14 de 35



PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Controle de Acesso - Conjunto de procedimentos, recursos e meios utilizados com a finalidade de garantir que os acessos aos ativos só ocorrerão após autorização e serão restritos, baseados nos requisitos de segurança e nas atividades do usuário.

Credenciais ou Contas de Acesso - Identificação única, concedida de forma pessoal e intransferível a uma pessoa, em conjunto com um método de autenticação. Esse par de informações habilita o seu dono a acessar equipamentos, sistemas e aplicações específicas, de acordo com o perfil definido.

Classificação da Informação - Identificação do nível de proteção requerido pela informação, atribuído por autoridade competente.

Confidencialidade - Nenhuma informação estará disponível ou será divulgada a entidades (pessoas, sistemas ou órgãos) não autorizadas.

Colaborador - Servidores públicos efetivos, contratados por tempo determinado ou comissionados; estagiários; prestadores de serviço; visitantes; ou, ainda, quaisquer usuários externos do sistema de informação da Prefeitura Municipal de Reginópolis.

Críticidade - Medida de risco obtida da combinação entre o possível impacto na Instituição ou em um projeto e a probabilidade de ocorrência de um evento que os afete.

Custodiante do Ativo - Unidade administrativa responsável pelo armazenamento, pela operação, administração e preservação de ativos.

Custodiante da Informação - Colaborador responsável pela guarda adequada do dado.

Divulgação - Ato de tornar público o resultado de uma informação.

Equipe de Tratamento de Incidentes - Grupo de pessoas com a responsabilidade de analisar, tratar e documentar os incidentes de segurança nas redes de computadores, e o tratamento aplicado.

Gestor - Unidade administrativa responsável por gerenciar determinado segmento de dados e todos os ativos relacionados.

Incidente - Um ou mais eventos indesejados ou inesperados que podem causar algum dano, colocando em risco os ativos de informação, com probabilidade de interromper ou afetar a qualidade dos serviços e/ou atividades da Instituição.

Infraestrutura de Tecnologia da Informação - Instalações prediais, equipamentos, computadores, *software*, redes, telecomunicações, sistemas de



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 15 de 35



PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

armazenamento e recuperação de dados, aplicações computacionais, cabeamento e rede telefônica.

Mitigar/Reduzir o risco - Efetuar ações que reduzam a probabilidade, consequências negativas, ou ambas, associadas a um risco.

PDTI - Plano Diretor de Tecnologia da Informação.

PMR - Prefeitura Municipal de Reginópolis.

Política - Intenções e diretrizes da organização, formalmente expressas pela direção da Instituição.

PSI - Política de Segurança da Informação.

Risco - Efeito da incerteza sobre os objetivos de segurança da informação associado com o potencial de que as ameaças explorem vulnerabilidades de um ativo de informação ou grupo de ativos de informação e, assim, causar danos a uma organização.

Segurança da Informação - Preservação da confidencialidade, da integridade e da disponibilidade das informações.

Sigilo - Confidencialidade, segredo.

TI - Tecnologia da Informação.

Transferir o risco - Compartilhamento com uma outra entidade do ônus da perda ou do benefício do ganho associado a um risco.

Vulnerabilidade - Fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças.

VPN - (Rede Privada Virtual) - é uma tecnologia que cria uma conexão segura e criptografada entre o usuário e um servidor remoto.

3. Objetivos da Política de Segurança da Informação (PSI)

A PSI visa proteger a integridade, disponibilidade e confidencialidade das informações custodiadas pela Prefeitura Municipal de Reginópolis, promovendo uma cultura organizacional que prioriza a segurança.

Objetivos Específicos:

3.1. Estabelecer diretrizes para a segurança das informações.

3.2. Promover um comportamento ético no uso das ferramentas tecnológicas.



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 16 de 35



PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

4. Princípios

Atualidade - As normas e procedimentos devem ser constantemente atualizados, de modo a refletir as mudanças legais, sociais e tecnológicas que interferem na sua aplicabilidade;

Aplicabilidade - Os processos de segurança devem ser coordenados e integrados entre si e incorporados nos processos de trabalho e práticas de todas as unidades da Prefeitura Municipal de Reginópolis;

Autenticidade - Toda informação terá sua origem certificada;

Clareza - Todas as normas e procedimentos de segurança produzidos devem ser claros o suficiente para que todos os envolvidos com a informação entendam as suas responsabilidades, bem como os seus direitos e limites;

Conhecimento - Os servidores devem ser continuamente capacitados para o desenvolvimento da cultura de segurança da informação;

Confidencialidade - Nenhuma informação estará disponível ou será divulgada a entidades (pessoas, sistemas ou órgãos) não autorizadas;

Disponibilidade - Toda informação estará disponível e poderá ser utilizada sob demanda por entidade autorizada (pessoa, sistema ou órgão);

Integridade - Os ativos de informação deverão ser protegidos, garantindo que só sejam alterados de forma autorizada e não acidental.

5. Diretrizes

As diretrizes devem ser seguidas por todos os colaboradores e qualquer pessoa que tenha acesso às informações.

Diretrizes Específicas:

- 5.1. Propriedade das informações geradas.
- 5.2. Manutenção dos mecanismos de proteção.
- 5.3. Reavaliação periódica das ameaças e riscos.
- 5.4. Limitação do acesso às informações conforme as atribuições.
- 5.5. Reflexão da PSI nos processos de aquisição.



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 17 de 35



PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

6. Responsabilidades

6.1 Colaboradores

Cada colaborador é responsável por seguir as diretrizes e normas estabelecidas na PSI.

6.2 Gestores de Pessoas e/ou Processos

Os gestores devem servir como modelos em relação à segurança da informação e garantir que todos os colaboradores assinem o Termo de Ciência e Compromisso.

6.3 Setor de Recursos Humanos

Informar ao setor de TI sobre desligamentos para bloquear acessos;
Entrega de uma cópia do Termo de Ciência de Responsabilidade bem como a coleta do termo assinado.

6.4 Custodiantes da Informação (Área de Tecnologia da Informação)

Devem garantir a configuração adequada dos sistemas para cumprir os requisitos desta PSI.

7. Políticas

7.1 Controle de Acesso Lógico

O controle de acesso lógico é fundamental para garantir a segurança das informações na Prefeitura Municipal de Reginópolis (PMR). As diretrizes a seguir devem ser rigorosamente seguidas:

7.1.1 Conta de Acesso

Cada usuário possui uma conta de acesso individual aos sistemas, que é o principal meio de identificação. O compartilhamento dessa conta é estritamente proibido, e o responsável pela conta responde por todas as ações realizadas com ela.

7.1.2 Princípio do Privilégio Mínimo

A concessão de privilégios de acesso deve respeitar o princípio do privilégio mínimo, ou seja, cada credencial deve ter apenas os direitos necessários para o desempenho das funções atribuídas ao usuário.

7.1.3 Acesso Remoto

O acesso remoto a ativos de tecnologia da informação requer autorização do custodiante do ativo, após análise da justificativa apresentada pelo gestor. Esse acesso deve ser limitado aos ativos necessários, utilizar canais seguros e ser concedido em caráter provisório.



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 18 de 35



PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

7.1.4 Solicitação de Acesso

Os gestores são responsáveis por solicitar, via ofício ou e-mail corporativo, a concessão de acesso aos sistemas e por informar imediatamente quaisquer alterações nas atribuições dos colaboradores para adequar os privilégios de acesso.

7.1.5 Senhas de Usuários

As senhas para autenticação nos sistemas da PMR devem seguir critérios mínimos:

Complexidade: Mínimo de 6 caracteres, incluindo letras (maiúsculas e minúsculas), números e caracteres especiais (@ # \$ %).

Segurança: Não devem ser baseadas em informações pessoais.

Expiração: Devem ser alteradas periodicamente, preferencialmente a cada 90 dias; senhas não alteradas poderão ser bloqueadas.

Troca Inicial: A troca de senha é obrigatória no primeiro login (se for gerada senha temporária).

Não compartilhamento: As senhas são de uso particular e não devem ser compartilhadas.

7.1.6 Recuperação de Senha

Caso um colaborador esqueça sua senha, ele deve solicitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrá-la novamente.

7.1.7 Comunicação de Anomalias

Qualquer anormalidade percebida em relação aos privilégios de acesso deve ser imediatamente comunicada à equipe de Tecnologia da Informação.

7.1.8 Contas Administrativas

As contas com privilégios administrativos devem ser utilizadas exclusivamente para atividades relacionadas à administração do ambiente, e as credenciais necessárias para esse acesso devem ser restritas aos administradores dos equipamentos/sistema.

7.2 Controle de Acesso à Infraestrutura

7.2.1 O acesso ao datacenter

É restrito aos funcionários do setor de TI, o acesso por terceiros, como prestadores de serviço, deverá sempre ser acompanhado de um funcionário do setor. O mesmo se aplica a funcionários de outros setores.

7.2.2 A porta de acesso

A porta de acesso ao datacenter e *racks* devem permanecer fechadas, mesmo quando houver funcionários autorizados em suas dependências.

7.3 Controle de Acesso à Internet



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 19 de 35



PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

7.3.1 Uso Permitido

As áreas, serviços e conteúdos da PMR não podem ser utilizados para fins ilegais ou proibidos por esta Política de Uso, evitando danos, desativação ou interferência no uso por outros colaboradores. O acesso não autorizado a sistemas ou redes é estritamente proibido.

7.3.2 Uso Profissional

O acesso à rede corporativa, computadores, Internet e e-mail corporativo deve ser exclusivamente para fins profissionais. Qualquer uso pessoal deve ter autorização expressa do superior hierárquico.

7.3.3 Monitoramento

A PMR possui em seus sistemas registros das ações de uso e monitoramento dos arquivos institucionais através da rede local e das estações de trabalho. A inspeção das estações de trabalho e arquivos armazenados pode ocorrer sem aviso prévio para garantir o cumprimento desta política.

7.3.4 Restrições de Acesso

O acesso à Internet para fins pessoais pode ser bloqueado sem aviso prévio ao colaborador. É proibido acessar sites que contenham material sexualmente explícito, ofensivo, apologia à violência ou drogas, violação de direitos autorais, fraudes ou compartilhamento não autorizado de arquivos.

7.3.5 Proibições Específicas

7.3.5.1 Troca de Arquivos: Não é permitido trocar arquivos de vídeo ou música, exceto se relacionados às atividades do colaborador.

7.3.5.2 O uso de dispositivos de armazenamento removíveis, como pen drives, HDs externos, cartões de memória e similares, é permitido nos equipamentos e sistemas da instituição, desde que realizado com responsabilidade e em conformidade com as diretrizes de segurança da informação. O usuário deve estar ciente dos riscos relacionados a infecção por vírus, perda de dados e vazamento de informações sensíveis. O uso inadequado desses dispositivos poderá acarretar responsabilização administrativa, civil ou penal, sendo de inteira responsabilidade do usuário qualquer dano causado aos sistemas institucionais ou vazamento de dados.

Recomenda-se que, sempre que possível, seja priorizado o uso de recursos internos como o Servidor de Arquivos ou sistemas oficiais da instituição.

7.3.5.3 Transferência de Programas: A transferência de programas para a rede interna da PMR requer autorização específica.

7.3.5.4 Downloads Restritos: Downloads de arquivos com extensões específicas (ex.: .exe, .mp3, .bat) são proibidos, exceto se relacionados às atividades do colaborador.

7.3.5.5 Conteúdo sob Demanda: O acesso a programas de TV na Internet ou serviços de streaming é proibido.



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 20 de 35



PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

7.3.6 Uso do E-mail Corporativo

O e-mail corporativo é uma ferramenta da PMR e não confere direito sobre seu conteúdo a terceiros. Informações confidenciais não devem ser divulgadas fora do âmbito profissional.

7.3.7 Responsabilidade pela Informação

Colaboradores que divulgarem informações confidenciais em qualquer meio poderão enfrentar penalidades conforme as políticas internas ou a legislação vigente.

7.3.8 Atividades Ilegais

Qualquer uso dos recursos da PMR para atividades ilegais pode resultar em penalidades severas, incluindo Processo Administrativo Disciplinar.

7.3.9 Equipamentos Pessoais

A entrada e uso de equipamentos pessoais (smartphones, tablets) devem ser comunicados à PMR, que não se responsabiliza por danos ou perdas.

7.3.10 Disponibilidade da Política

Esta Política estará disponível em formato virtual para conhecimento dos colaboradores, sendo que o desconhecimento não exime responsabilidades.

7.3.11 Dúvidas e Comentários

Colaboradores com dúvidas sobre esta Política devem contatar seu responsável ou o Setor de Tecnologia da Informação.

7.4 E-mail Corporativo

7.4.1 Uso do Domínio Corporativo

O uso do e-mail deve ser restrito ao domínio @reginopolis.sp.gov.br. É proibido a utilização de domínios não corporativos.

7.4.2 Atividades Ilegais

É vedado praticar crimes ou infrações de qualquer natureza através do e-mail corporativo.

7.4.3 Ações Nocivas

Os colaboradores não devem executar ações que possam prejudicar os recursos computacionais da PMR ou de redes externas.

7.4.4 Conteúdo Inapropriado

É proibido distribuir material obsceno, pornográfico, ofensivo, preconceituoso ou discriminatório, bem como qualquer conteúdo contrário à lei e aos bons costumes.



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 21 de 35



PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

7.4.5 Anúncios e Mensagens Indesejadas

Não é permitido disseminar anúncios publicitários, mensagens de entretenimento, correntes, vírus ou programas que não estejam relacionados ao desempenho das funções.

7.4.6 Envio de Arquivos

O envio de arquivos de áudio, vídeo ou animações é permitido apenas se relacionado às funções institucionais desempenhadas pela PMR.

7.4.7 Divulgação de Contatos

A divulgação dos endereços eletrônicos corporativos do catálogo de endereços do serviço é vedada.

7.4.8 Vulnerabilidade Legal

Os colaboradores não devem enviar mensagens que possam tornar o remetente ou a PMR vulneráveis a ações civis ou criminais.

7.4.9 Informações Confidenciais

É proibido divulgar informações não autorizadas, imagens de tela, sistemas ou documentos sem autorização expressa do proprietário da informação.

7.4.10 Atividades Lesivas

Qualquer atividade que comprometa a intimidade dos usuários ou a segurança do sistema é estritamente proibida.

7.4.11 Responsabilidades do Usuário

7.4.11.1 Sigilo da Senha

Os usuários devem manter em sigilo suas senhas de acesso ao correio eletrônico.

7.4.11.2 Fechamento do Aplicativo

É obrigatório fechar o aplicativo de correio sempre que o usuário se ausentar, evitando acessos indevidos.

7.4.13 Comunicação de Vírus

Qualquer recebimento de mensagens com vírus ou que possam causar danos aos sistemas deve ser comunicado imediatamente ao Setor de Tecnologia da Informação.

7.4.14 Manutenção da Caixa Postal

Os usuários devem gerenciar suas caixas postais, avisando ao Setor de Tecnologia da Informação caso necessite de aumento de armazenamento. Mantendo assim, o funcionamento contínuo do serviço.

7.5 Uso de Equipamentos de Informática

O objetivo desta seção é estabelecer critérios para a utilização dos equipamentos de informática na Prefeitura Municipal de Reginópolis. As diretrizes a seguir devem ser seguidas rigorosamente:



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 22 de 35



PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

7.5.1 Uso Exclusivo

Os recursos computacionais devem ser utilizados exclusivamente para atividades de interesse da PMR.

7.5.2 Identificação da Estação de Trabalho

Cada estação de trabalho possui controle de IP, permitindo sua identificação na rede.

7.5.3 Proibições de Gravação

É proibido armazenar arquivos de mídia, como músicas (MP3), filmes, fotos de cunho pessoal, bem como *softwares* protegidos por direitos autorais, nas estações de trabalho e na rede da Prefeitura Municipal de Reginópolis (PMR), salvo mediante autorização expressa.

7.5.4 Armazenamento de Dados

Todos os dados relacionados às atividades da Secretaria devem ser mantidos no Servidor de Arquivos, que possui backup. Quando o Servidor não estiver disponível, o usuário deve realizar cópias de segurança dos arquivos locais e eliminar dados desnecessários.

7.5.5 Cópia de Segurança

Não será feita cópia de segurança dos arquivos criados no computador local dos colaboradores; é responsabilidade do usuário manter suas cópias.

7.5.6 Reparo de Equipamentos

A abertura de computadores para reparos é proibida; qualquer necessidade deve ser encaminhada ao suporte técnico do setor de Tecnologia da Informação.

7.5.7 Equipamentos Pessoais

O uso de equipamentos pessoais, como celulares, notebooks e dispositivos similares, nas dependências da instituição ou em atividades laborais, deverá ser previamente comunicado à chefia imediata, que deliberará sobre a autorização de uso conforme a necessidade e pertinência.

A área de Tecnologia da Informação não se responsabiliza por quaisquer problemas, danos ou prejuízos decorrentes do uso inadequado desses equipamentos, incluindo, mas não se limitando a, falhas de segurança, perda de dados ou comprometimento da rede institucional.

Cabe ao usuário garantir que o uso de dispositivos pessoais esteja em conformidade com as normas de segurança da informação vigentes.

7.5.8 Comunicação de Danos

Em caso de dano, inutilização ou extravio do equipamento, o colaborador deve comunicar imediatamente o setor de Tecnologia da Informação.



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 23 de 35



PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

7.5.9 Furto ou Roubo

Em caso de furto ou roubo, o colaborador deve registrar um Boletim de Ocorrência junto à Polícia Civil e entregá-lo à chefia imediata, com cópia ao setor de Tecnologia da Informação.

7.5.10 Adesivos e Modificações

É proibido colocar adesivos magnéticos nos equipamentos e danificar placas identificadoras ou lacres de segurança.

7.5.11 Zelo pelo Equipamento

Os colaboradores devem zelar pela integridade dos equipamentos e acessórios utilizados como instrumentos de trabalho.

7.5.12 Verificação do Termo de Responsabilidade

Ao receber o Termo de Responsabilidade, o colaborador deve verificar as informações contidas nele.

7.5.13 Configurações do Equipamento

Não é permitido alterar configurações da rede ou da BIOS das máquinas sem autorização.

7.5.14 Uso Não Autorizado

É vedado o uso dos equipamentos por pessoas sem vínculo com a PMR sem autorização prévia.

7.5.15 Conexão à Rede

A conexão ou configuração de equipamentos à rede deve ser autorizado pelo chefe imediato ou pelo Setor de Tecnologia da Informação.

7.5.16 Antivírus Atualizado

Os antivírus devem estar atualizados e com a autoproteção ativa nas estações de trabalho.

7.5.17 Armazenamento Seguro

Equipamentos críticos devem ser armazenados em áreas apropriadas com acesso restrito.

7.5.18 Acesso às Áreas Críticas

O acesso a áreas que hospedam equipamentos críticos deve ser autorizado pelo custodiado e acompanhado por um servidor público.

7.5.19 Uso Exclusivo dos Notebooks

Os notebooks devem ser utilizados exclusivamente para atividades profissionais relacionadas ao Município.



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 24 de 35



PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

7.5.20 Restrições no Uso do Notebook

A utilização do notebook fora das dependências da PMR só é permitida diante a autorização do superior hierárquico.

7.5.21 Armazenamento Pessoal

Arquivos pessoais não podem ser armazenados no notebook e podem ser excluídos sem aviso prévio durante formatações realizadas pelo setor técnico.

7.5.22 Zelo pelos Equipamentos de Informática

Os colaboradores devem cuidar do bom uso dos equipamentos de informática, evitando danos e quaisquer avarias nos mesmos.

7.5.23 Reposição por Mau Uso ou Perda

Para reposição dos equipamentos de informática por mau uso ou perda, o valor a ser pago será equivalente ao que consta na nota fiscal, atualizado pelo índice INPC/IBGE.

7.6 Backups

O objetivo desta seção é estabelecer diretrizes para a realização de backups na Prefeitura Municipal de Reginópolis, assegurando a integridade e disponibilidade das informações. As diretrizes a seguir devem ser seguidas:

7.6.1 Automatização dos Backups

Todos os backups devem ser automatizados por sistemas de agendamento, preferencialmente executados fora do horário comercial, durante as "janelas de backup", quando há pouco ou nenhum acesso aos sistemas.

7.6.2 Gestão de Sistemas de Backup

Os colaboradores responsáveis pela gestão dos sistemas de backup devem realizar pesquisas frequentes para identificar atualizações, novas versões, ciclo de vida do software e sugestões de melhorias.

7.6.3 Monitoramento dos Backups

Os backups devem ser monitorados para excluir aqueles que apresentem inviabilidade técnica e ultrapassem o prazo recomendado de guarda.

7.7 Auditoria, monitoramento e registro de logs de acesso

Para garantir o cumprimento das diretrizes estabelecidas nesta Política de Segurança da Informação, a Prefeitura Municipal de Reginópolis poderá adotar as seguintes medidas:

7.7.1 Implantação de Sistemas de Monitoramento

A PMR implantará sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a Internet, dispositivos móveis e outros componentes da rede. As informações geradas por esses sistemas poderão ser



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 25 de 35



PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

utilizadas para identificar usuários, acessar registros e monitorar materiais manipulados.

7.7.2 Divulgação de Informações

As informações obtidas pelos sistemas de monitoramento e auditoria poderão ser tornadas públicas em caso de exigência judicial ou solicitação da chefia ou superior.

7.7.3 Inspeção Física

A PMR reserva-se o direito de realizar inspeções físicas a qualquer momento nas máquinas sob sua propriedade.

7.7.4 Sistemas de Proteção

Serão instalados sistemas de proteção, tanto preventivos quanto detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

7.7.5 Registro Automático de Credenciais

As credenciais de acesso serão registradas em logs automáticos, abrangendo todos os acessos dos usuários aos recursos da instituição. Isso incluirá acessos aos sistemas, criação, exclusão e alteração de arquivos, horários de login nas máquinas, utilização de impressoras e outros sistemas.

7.8 Política de Uso de Impressoras

A utilização das impressoras na Prefeitura Municipal de Reginópolis deve ser feita de forma responsável e consciente, visando a eficiência operacional e a sustentabilidade ambiental. As diretrizes a seguir devem ser seguidas e poderão ser implementadas para controle:

7.8.1 Registro de Impressões

Todas as impressões realizadas poderão ser registradas em log, permitindo a auditoria quanto ao usuário que imprimiu, quantidade de páginas e nome do arquivo impresso.

7.8.2 Uso Exclusivo para Fins Institucionais

As impressoras devem ser utilizadas exclusivamente para atividades relacionadas aos interesses da PMR. O uso pessoal ou não autorizado é estritamente proibido.

7.8.3 Consciência Ecológica

Os colaboradores devem adotar práticas de impressão consciente, priorizando a impressão frente e verso e evitando impressões desnecessárias, contribuindo assim para a redução do consumo de papel.

7.8.4 Proibição de Impressão de Conteúdo Inadequado

É proibido imprimir materiais que contenham conteúdo ilegal, ofensivo ou que violem as políticas da PMR, incluindo, mas não se limitando a, material pornográfico, discriminatório ou que faça apologia à violência.



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 26 de 35



PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

7.8.5 Manutenção da Privacidade

Os colaboradores devem garantir que documentos confidenciais não sejam deixados nas impressoras após a impressão. É responsabilidade do usuário retirar imediatamente seus documentos e descartá-los adequadamente se não forem mais necessários.

7.8.6 Limitação de Acesso

O acesso às impressoras deve ser restrito aos colaboradores autorizados, evitando o uso indevido dos recursos.

7.8.7 Monitoramento e Auditoria

As impressoras poderão ser monitoradas quanto ao uso, e os logs de impressão poderão ser auditados periodicamente para garantir conformidade com esta política.

7.8.8 Responsabilidade pelo Equipamento

Os colaboradores são responsáveis pelo bom uso das impressoras e devem reportar imediatamente qualquer problema técnico ou necessidade de manutenção ao setor responsável.

7.9 Uso de Assinaturas Digitais

A Prefeitura Municipal de Reginópolis poderá, a seu critério, fornecer certificados digitais para usuários que desempenham atividades profissionais específicas. As seguintes diretrizes devem ser observadas:

7.9.1 Responsabilidade do Usuário

Conservação do Certificado: É de responsabilidade exclusiva do usuário a conservação de seu certificado digital, independentemente do equipamento que o suporte, bem como de qualquer tipo de senha ou meio de autenticação relacionado ao mesmo.

7.9.2 Comunicação de Incidentes

Notificação de Comprometimento: O usuário deve informar imediatamente ao seu superior hierárquico e à equipe de Tecnologia da Informação sobre quaisquer eventos ou suspeitas relativas ao comprometimento de sua senha e/ou ao uso indevido de seu certificado digital.

7.9.3 Revogação do Certificado

Desligamento ou Processo de Desligamento: O certificado digital expedido pela Prefeitura Municipal de Reginópolis será imediatamente revogado em caso de desligamento ou durante o processo de desligamento do usuário.



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 27 de 35



PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

7.10 Utilização do Sistema de CFTV

O acesso e a utilização do sistema de videomonitoramento (CFTV) da instituição estão condicionados à assinatura do Termo de Responsabilidade por Utilização de Câmeras de Segurança, documento específico que estabelece as condições de uso, sigilo e limites de acesso às imagens.

Somente servidores formalmente autorizados, após assinatura do termo e aprovação da chefia imediata e da autoridade competente, poderão acessar o sistema.

O descumprimento das disposições previstas no termo poderá resultar em sanções administrativas, civis e/ou penais, conforme a gravidade da infração.

7.11 Abertura de Chamados

Todas as solicitações de acesso remoto, reparos, visitas técnicas ou solicitações de insumos e dos sistemas, deverão ser feitas através obrigatoriamente do Sistema de Chamados.

8. Cumprimento

A Prefeitura Municipal de Reginópolis se reserva o direito de suspender o acesso de qualquer usuário que descumpra as regras estabelecidas nesta Política de Segurança da Informação (PSI), incluindo, mas não se limitando, ao uso excessivo dos recursos tecnológicos. A integridade e a ética são pilares fundamentais da cultura organizacional da Municipalidade; portanto, qualquer incidente de segurança será considerado uma violação dos princípios éticos e dos bons costumes que regem a Instituição.

O descumprimento das diretrizes desta política poderá resultar em auditorias a qualquer momento, conduzidas pela equipe de Tecnologia da Informação (TI). Dependendo da gravidade da infração, o usuário poderá enfrentar ações disciplinares apropriadas, que podem incluir advertências, suspensão ou ações mais rigorosas.

É imprescindível que todos os colaboradores compreendam a importância do cumprimento desta PSI não apenas como uma obrigação legal, mas como um compromisso coletivo para garantir a segurança das informações e a proteção dos ativos da Prefeitura Municipal de Reginópolis.

A colaboração e a responsabilidade individual são essenciais para manter um ambiente seguro e eficiente, onde todos possam desempenhar suas funções com confiança e integridade.

O comprometimento com as normas aqui estabelecidas é fundamental para a proteção dos dados e para a continuidade das operações da Instituição, refletindo o respeito mútuo e a responsabilidade compartilhada por todos os envolvidos.

9. Considerações Finais

A Política de Segurança da Informação (PSI) da Prefeitura Municipal de Reginópolis é um documento essencial que se aplica a todos os servidores e



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 28 de 35



PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

colaboradores que utilizam os recursos tecnológicos da PMR. Esta política abrange toda a infraestrutura de Tecnologia da Informação (TI) de todas as unidades municipais, estabelecendo diretrizes claras para garantir a segurança e a integridade das informações.

As políticas definidas nesta PSI devem ser amplamente divulgadas e promovidas entre todos os colaboradores, a fim de assegurar o comprometimento no uso correto dos recursos de TI disponibilizados pelo Município. A conscientização sobre a importância da segurança da informação é fundamental para criar uma cultura organizacional que valorize a proteção dos dados e minimize riscos potenciais.

Revisões periódicas devem garantir que a política permaneça atualizada e eficaz diante das constantes mudanças tecnológicas e das novas ameaças à segurança da informação.

A colaboração entre as diferentes unidades administrativas é crucial para o sucesso da implementação desta política, assegurando que todos os colaboradores estejam alinhados com as diretrizes estabelecidas.

Por fim, é imprescindível que cada colaborador compreenda sua responsabilidade individual na proteção das informações e no cumprimento das normas estabelecidas. A segurança da informação é uma tarefa coletiva, e o comprometimento de todos é vital para garantir um ambiente seguro e eficiente.



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 29 de 35



PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TERMO DE CIÊNCIA - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Objetivo

Definir as responsabilidades para todos os agentes públicos, estagiários e prestadores de serviços em atividade na Prefeitura Municipal de Reginópolis que tenham acesso aos recursos de tecnologia da informação ou à rede de computadores da instituição.

Pelo presente termo, declaro ter conhecimento da **Política de Segurança da Informação** da Prefeitura Municipal de Reginópolis, disponível para consulta no portal www.reginopolis.sp.gov.br no menu Secretarias – Administração Geral - Tecnologia da Informação – Política de Segurança da Informação, e concordo em aceitar suas regras.

Declaro estar ciente de que minhas ações podem ser monitoradas de acordo com a **Política de Segurança da Informação** e qualquer alteração feita sob minha identificação, advinda de minha autenticação e autorização, é de minha responsabilidade.

Estou ciente, ainda, de minha responsabilidade pelo dano que possa causar por descumprimento da **Política de Segurança da Informação** da Prefeitura Municipal de Reginópolis ao realizar uma ação de iniciativa própria de tentativa de modificação da configuração, física ou lógica, dos recursos computacionais sem a permissão da área competente.

Eu, _____, inscrito(a)
no CPF nº _____, **declaro** que li e estou ciente da
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO da Prefeitura Municipal de Reginópolis e
me **comprometo** a seguir todos os seus termos, bem como a me atualizar a respeito de
eventuais alterações.



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 30 de 35

DECRETO Nº. 064, DE 18 DE NOVEMBRO DE 2025.

“Institui o Município Digital, no âmbito da Administração Pública do Município de Reginópolis e dá outras providências”.

JEFFERSON AUGUSTO RODRIGUES BUAVA, Prefeito Interino de Reginópolis, Comarca de Pirajuí, Estado de São Paulo, usando das atribuições que lhe conferem a alínea “a”, inciso I, do artigo 85, da Lei Orgânica do Município,

D E C R E T A:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituído, no âmbito da Administração Pública do Município de Reginópolis, o Município Digital, com vistas à produção, gestão, tramitação, armazenamento, preservação, segurança e acesso a documentos e informações arquivísticas em ambiente digital de gestão documental.

Parágrafo único. A implantação do ambiente digital de gestão documental junto aos órgãos da Administração Pública dar-se-á gradualmente.

Art. 2º Para os fins deste decreto, consideram-se:

I - assinatura digital: modalidade de assinatura eletrônica que utiliza algoritmos de criptografia e permite aferir, com segurança, a origem e a integridade do documento;

II - assinatura eletrônica: geração, por computador, de símbolo ou série de símbolos executados, adotados ou autorizados por um indivíduo, com valor equivalente à assinatura manual do mesmo indivíduo, classificando-se em:

a) **assinatura eletrônica simples:** a que permite identificar o seu signatário e a que anexa ou associa dados a outros dados em formato eletrônico do signatário;

b) **assinatura eletrônica avançada:** a que utiliza certificados não emitidos pela ICP-Brasil ou outro meio de comprovação da autoria e da integridade de documentos em forma eletrônica, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento;

c) **assinatura eletrônica qualificada:** a que utiliza certificado digital, nos termos do § 1º do art. 10 da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

III - autenticidade: credibilidade de documento livre de adulteração;

IV - captura de documento: incorporação de documento nato-digital ou digitalizado por meio de registro, classificação e arquivamento em sistema eletrônico;

V - documento digital: documento codificado em dígitos binários, acessível e interpretável por meio de sistema computacional;

VI - documento digitalizado: documento obtido a partir da conversão de documento não digital, gerando uma fiel

representação em código digital, podendo ser capturado por sistemas de informação específicos;

VII - integridade: propriedade do documento completo e inalterado;

VIII - legibilidade: qualidade que determina a facilidade de leitura do documento;

IX - preservação digital: conjunto de ações gerenciais e técnicas de controle de riscos decorrentes das mudanças tecnológicas e fragilidade dos suportes, com vistas à proteção das características físicas, lógicas e conceituais dos documentos digitais pelo tempo necessário;

X - processo eletrônico: sucessão de atos registrados e disponibilizados em meio eletrônico, integrado por documentos nato-digitais ou digitalizados;

XI - processo híbrido: conjunto conceitualmente indivisível de documentos digitais e não digitais, reunidos em sucessão cronologicamente encadeada até sua conclusão.

Art. 3º São objetivos do Município Digital:

I - produzir documentos e processos eletrônicos com segurança, transparência, economicidade, sustentabilidade ambiental e, sempre que possível, de forma padronizada;

II - possibilitar maior eficácia e celeridade aos processos administrativos;

III - assegurar a proteção da autoria, da autenticidade, da integridade, da disponibilidade e da legibilidade de documentos digitais, observadas as disposições da Lei Federal nº 12.527, de 18 de novembro de 2011;

IV - assegurar a gestão, a preservação e a segurança de documentos e processos eletrônicos no tempo.

CAPÍTULO II

DA GESTÃO DE DOCUMENTOS

Art. 4º A gestão de documentos do Município de Reginópolis deve ser realizada exclusivamente por meio do memorando eletrônico, ofício eletrônico e protocolo eletrônico.

§ 1º A finalidade do **memorando eletrônico** é formalizar a gestão de documentos internos, quando se tratar de assuntos simples ou rotineiros, em especial:

I - solicitar execução de atividades;

II - solicitar compras;

III - agendar reuniões;

IV - solicitar informações;

V - encaminhar documentos;

VI - solicitar providências rotineiras;

VII - solicitar pareceres;

VIII - outros assuntos considerados de mero expediente.

§ 2º O **ofício eletrônico**, sobre qualquer assunto, expedido pelas autoridades dentro do sistema de gestão de documentos, serão encaminhados para destinatários fora da administração municipal por correio eletrônico, ficando sob responsabilidade do sistema a confirmação de entrega e leitura do documento.

§ 3º Os **protocolos** iniciados no âmbito do Município, serão gerados pelo requerente de forma eletrônica, ou



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 31 de 35

presencial na Secretaria competente, mediante exposição de motivos e juntada de documentos que o fundamentem.

Art. 5º Todos os documentos eletrônicos, bem como seus anexos, recebem obrigatoriamente uma numeração sequencial automática e passam a circular dentro dos setores competentes.

Parágrafo único. A responsabilidade pela guarda excessiva ou pelo descarte indevido dos documentos, sejam eletrônicos ou impressos, é da unidade emissora.

Art. 6º Fica vedada a impressão de documentos eletrônicos, exceto para:

I - fornecer comprovante ao requerente que efetuou o protocolo de forma presencial;

II - impressão do documento, na forma da legislação que a exigir.

III - juntar a processo administrativo, quando o assunto exigir a juntada do documento.

Parágrafo único. A exceção prevista no inciso III deste artigo ficará sob a responsabilidade do agente público que juntou o documento no processo administrativo.

Art. 7º A classificação da informação sigilosa e a proteção de dados pessoais no ambiente digital de gestão documental observarão as disposições da Lei federal nº 12.527, de 18 de novembro de 2011 e das demais normas aplicáveis.

Art. 8º A autoria, a autenticidade e a integridade de documentos digitais e da assinatura poderão ser obtidas por meio de certificação digital emitida conforme padrões definidos pela Infraestrutura de Chaves Públicas Brasileira - ICP - Brasil, instituída pela Medida Provisória nº 2.200-2, de 24 de agosto de 2001, assim como pelo uso de assinatura eletrônica, nos termos da Lei 14.063, de 23 de setembro de 2020, preservadas as hipóteses legais de anonimato.

§ 1º O disposto no caput deste artigo não obsta a utilização de outro meio lícito de comprovação da autoria, autenticidade e integridade de documentos digitais, em especial aqueles que utilizem identificação por meio de usuário e senha.

§ 2º Os documentos nato-digitais assinados eletronicamente na forma deste artigo serão considerados originais nos termos da lei aplicável.

Art. 9º Os atos processuais praticados no ambiente digital de gestão documental deverão observar os prazos definidos em lei para manifestação dos interessados e para decisão da autoridade competente, sendo considerados realizados na data e horário identificados no recibo eletrônico de protocolo emitido pelo sistema.

§ 1º Salvo disposição legal ou regulamentar em contrário, o ato a ser praticado em prazo determinado será considerado tempestivo se realizado até as vinte e três horas e cinquenta e nove minutos do último dia do prazo, no horário oficial de Brasília.

§ 2º Na hipótese prevista no § 1º deste artigo, caso o sistema se torne indisponível por motivo técnico, o prazo será automaticamente prorrogado até as vinte e três horas e cinquenta e nove minutos do primeiro dia útil seguinte ao

do retorno da disponibilidade.

§ 3º Usuários não cadastrados no ambiente digital de gestão documental terão acesso, na forma da lei, a documentos e processos eletrônicos por meio de arquivo em formato digital, disponibilizado pelo órgão da Administração Pública detentor do documento.

CAPÍTULO III

DAS ASSINATURAS ELETRÔNICAS E FORNECIMENTO DE ACESSO

Art. 10. Sem prejuízo de interações em que se admite o anonimato, os níveis mínimos para as assinaturas em interações eletrônicas com a Administração Municipal, são:

I - **assinatura simples:** admitida para as hipóteses cujo conteúdo da interação não envolva informações protegidas por grau de sigilo e não ofereça risco direto de dano a bens, serviços e interesses do ente público, incluídos:

a) a solicitação de agendamentos, atendimentos, anuências, autorizações e licenças para a prática de ato ou exercício de atividade;

b) a realização de autenticação ou solicitação de acesso a sítio eletrônico oficial que contenha informações de interesse particular, coletivo ou geral, mesmo que tais informações não sejam disponibilizadas publicamente;

c) o envio de documentos digitais ou digitalizados e o recebimento de número de protocolo decorrente da ação;

d) a participação em pesquisa pública; e

II - **assinatura eletrônica avançada:** admitida para as hipóteses previstas no inciso I e nas hipóteses de interação com o ente público que, considerada a natureza da relação jurídica, exijam maior garantia quanto à autoria, incluídos:

a) as interações eletrônicas entre pessoas naturais ou pessoas jurídicas de direito privado e os entes públicos que envolvam informações classificadas ou protegidas por grau de sigilo;

b) os requerimentos de particulares e as decisões administrativas;

c) a manifestação de vontade para a celebração de contratos, convênios, acordos, termos e outros instrumentos sinalagmáticos bilaterais ou plurilaterais congêneres;

d) os atos relacionados a auto cadastro, como usuário particular ou como agente público, para o exercício de atribuições, em sistema informatizado de processo administrativo eletrônico ou de serviços;

e) as decisões administrativas referentes à concessão de benefícios assistenciais, trabalhistas e tributários que envolvam dispêndio direto ou renúncia de receita pela administração pública;

f) as declarações prestadas em virtude de lei que constituam reconhecimento de fatos e assunção de obrigações;

g) o envio de documentos digitais ou digitalizados em atendimento a procedimentos administrativos ou medidas de fiscalização; e



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 32 de 35

h) a apresentação de defesa e interposição de recursos administrativos; e

III - **assinatura eletrônica qualificada**: aceita em qualquer interação eletrônica com entes públicos e obrigatória para:

a) os atos assinados pelo Chefe do Executivo e Secretários Municipais; e

c) as demais hipóteses previstas em lei.

§ 1º A autoridade máxima do órgão ou da entidade poderá estabelecer o uso de assinatura eletrônica em nível superior ao mínimo exigido no **caput**, caso as especificidades da interação eletrônica em questão o exijam.

§ 2º A exigência de níveis mínimos de assinatura eletrônica não poderá ser invocada como fundamento para a não aceitação de assinaturas realizadas presencialmente ou derivadas de procedimentos presenciais para a identificação do interessado.

§ 3º A assinatura simples de que trata o inciso I do **caput** será admitida para interações eletrônicas em sistemas informatizados de processo administrativo ou de atendimento a serviços públicos, por parte de agente público, exceto nas hipóteses em que se exigir assinatura eletrônica qualificada.

Art. 11. A Administração Municipal adotará mecanismos para prover aos usuários a capacidade de utilizar assinaturas eletrônicas para as interações com entes públicos, respeitados os seguintes critérios:

I - para a utilização de assinatura simples, o usuário poderá fazer seu cadastro pela internet, mediante autodeclaração validada em bases de dados governamentais;

II - para a utilização de assinatura avançada, o usuário deverá realizar o cadastro com garantia de identidade a partir de validador de acesso digital, incluída a:

a) validação biográfica e documental, presencial ou remota, conferida por agente público; ou

b) validação biométrica conferida em base de dados governamental; ou

c) validação biométrica, biográfica ou documental, presencial ou remota, conferida por validador de acesso digital que demonstre elevado grau de segurança em seus processos de identificação; e

III - para utilização de assinatura qualificada, o usuário utilizará certificado digital, nos termos da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

CAPÍTULO III

DAS CAIXAS DE MENSAGENS

Art. 12. O envio e recebimento dos documentos eletrônicos será feito exclusivamente pelo sistema adotado pelo Município.

Art. 13. O titular do órgão terá acesso a caixa de mensagens da unidade que dirige, por meio de login no sistema, sendo de sua responsabilidade:

I - manter em sigilo a senha de acesso ao sistema;

II - delegar acesso a outros servidores públicos à caixa

de mensagens da unidade;

III - efetuar log-off, sempre que se ausentar da unidade, a fim de evitar acesso indevido;

IV - comunicar aos membros do Comitê de Tecnologia da Informação sobre a utilização indevida da caixa da unidade;

V - zelar:

a) pela fidelidade dos dados enviados e pelo envio ao destinatário certo;

b) pelo acesso ao conteúdo armazenado na caixa;

c) pela leitura dos documentos recebidos;

d) pela guarda ou descarte de mensagens enviadas, recebidas e de controle;

e) pela resposta ou encaminhamento da demanda remetida ao setor competente via documento eletrônico.

CAPÍTULO IV

DA EMPRESA CONTRATADA

Art. 14. À Empresa contratada para o fornecimento de solução tecnológica cabe o desenvolvimento, a implantação, o processamento e o fornecimento do suporte tecnológico necessário para o Município Digital, bem como a orientação às áreas de tecnologia da informação junto aos órgãos da Administração Pública, para a utilização e a manutenção do ambiente digital de gestão documental.

§ 1º Poderá ser adotada soluções de mercado, em modelo de licenciamento, escolhidas com observância das normas de licitações, cujo contratado será responsável pelo fornecimento da licença, assim como suporte, orientações e *backups* - cópia de segurança dos documentos.

§ 2º Fica a empresa contratada responsável pelo treinamento e disponibilização de vídeos tutoriais para treinamento dos servidores.

CAPÍTULO V

DAS ATRIBUIÇÕES DO COMITÊ DE TECNOLOGIA DA INFORMAÇÃO

Art. 15. Ao Comitê de Tecnologia da Informação caberão as atribuições complementares:

I - promover estudos para a aplicação de tecnologias da informação às atividades de produção, gestão, preservação, segurança e acesso aos documentos e informações arquivísticas;

II - propor a edição de normas que se fizerem necessárias para o ambiente digital de gestão documental, em especial atinente à assinatura simples, assinatura avançada e assinatura qualificada quanto ao validador de acesso digital;

III - propor metodologia e orientar os órgãos e entidades da Administração Pública no processo de modelagem de documentos digitais e na definição de padrões de formato e conteúdo;

IV - propor e zelar pela observância das regras de negócio na parametrização e aprimoramento tecnológico de soluções;

V - apoiar as atividades e organizar o expediente da Comissão do Município Digital.

CAPÍTULO VI



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 33 de 35

DA COMISSÃO DO MUNICÍPIO DIGITAL

Art. 16. Fica instituída a Comissão do Município Digital com as seguintes atribuições:

I - propor políticas, estratégias, ações, procedimentos e técnicas de preservação e segurança digital;

II - assegurar a implantação, gestão, manutenção e atualização contínua do ambiente digital de gestão documental;

III - controlar os riscos decorrentes da degradação do suporte, da obsolescência tecnológica e da dependência de fornecedor ou fabricante;

IV - fixar diretrizes e parâmetros a serem observados nos procedimentos de implantação e manutenção do Programa;

V - promover a articulação e alinhamento de ações estratégicas relativas ao Programa, em conformidade com a política municipal de arquivos e gestão documental;

VI - analisar propostas apresentadas por órgãos da Administração Pública, relativas ao ambiente digital de gestão documental, emitindo parecer técnico conclusivo;

VII - disciplinar a produção de documentos ou processos híbridos e aprovar os critérios técnicos a serem observados no procedimento de digitalização;

VIII - manifestar-se, quando provocado, sobre hipóteses não disciplinadas neste decreto, relativas ao ambiente digital de gestão documental.

Art. 17. A Comissão do Município Digital será integrada por representantes e respectivos suplentes designados pelo Chefe do Poder Executivo, na seguinte conformidade:

I - 3 (três) da Secretaria Municipal da Administração Geral;

§ 1º A Comissão do Município Digital poderá convidar especialistas de órgãos e entidades da Administração Pública para, sem prejuízo de suas atribuições na origem, contribuir no desenvolvimento de ações ou projetos específicos.

§ 2º A participação na Comissão do Município Digital, de que trata este artigo, não será remunerada, mas considerada serviço público relevante.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 18. A implantação do ambiente digital de gestão documental junto aos órgãos da Administração Pública dar-se-á gradualmente, obedecendo a seguinte ordem cronológica:

I - Implantação do gestor de documentos digitais interno, conforme previsto nos parágrafos do Art. 4º desse decreto, far-se-á gradualmente, até a data de **01 de março de 2026**, iniciando-se em **01 de janeiro de 2026**.

II - Implantação do Protocolo Digital, liberação de aplicativo móvel e acesso aos munícipes, far-se-á gradualmente, com previsão de conclusão até o dia **01 de março de 2026**.

Parágrafo único. Após os prazos citados, todas as tramitações de documentos internos e externos serão de

forma eletrônica, não aceitando em hipótese alguma, requisições em formato físico.

Art. 19. Será vedada a utilização de documentos impressos nos casos abrangidos por este Decreto.

Art. 20. Compete a cada unidade administrativa orientar os usuários quanto à implementação da comunicação eletrônica no Município.

Art. 21. As despesas decorrentes da execução deste decreto correrão por conta das dotações orçamentárias próprias, suplementares se necessário.

Art. 22. Este Decreto entra em vigor na data de sua publicação.

Reginópolis, 18 de novembro de 2025.

JEFFERSON AUGUSTO RODRIGUES BUAVA

Prefeito Municipal

Registrado na Secretaria e publicado na forma da Lei vigente.

.....



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 34 de 35

Outros atos oficiais



PREFEITURA MUNICIPAL DE REGINÓPOLIS

SECRETARIA MUNICIPAL DE EDUCAÇÃO

LISTA DE ESPERA – Creche, Pré-Escola e Ensino Fundamental



A Secretaria Municipal de Educação do município de Reginópolis, obedecendo a **Lei nº 14.685 de 20 de setembro de 2023**, que acrescenta dispositivo à Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), para determinar ao poder público a obrigação de divulgar a lista de espera por vagas nos estabelecimentos de educação básica de sua rede de ensino, DIVULGA a Lista de Espera das Unidades Escolares Creche Escola "Profª Fanny Dyna Martins", Creche Escola "Profª Celina Lucia Soares Martins e EMEF Profª Regina Olinda Martins Ferro.

MICHELI ULIAN SILVA CAMARGO, Secretária Municipal de Educação de Reginópolis-SP, no uso e gozo de suas atribuições que lhe são conferidas por lei, de acordo com informações fornecidas pelas Diretoras das respectivas Unidades Escolares, DECLARA que o município POSSUI lista de espera de alunos na modalidade Creche, na C.E.M Profª Celina Lúcia Soares Martins, relacionadas abaixo. Nas outras unidades NÃO possui lista de espera.

BERÇÁRIO I

Posição	Nome	Data de Nascimento
01	M.F.S	24/04/2025
02	J.H.O.S	22/09/2025
03	E.H.O.M	25/05/2024

Os alunos M.E.S e E.H.O.M, já se encontram matriculados na Creche-Escola Fanny Dyna Martins, porém aguardam vaga na Creche-Escola Celina Lúcia Soares Martins.

MATERNAL I

Posição	Nome	Data de Nascimento
01	K.F.A.S	18/07/2022

A aluna já se encontra matriculada na Creche-Escola Fanny Dyna Martins, porém aguarda vaga na Creche-Escola Celina Lúcia Soares Martins.

Reginópolis, 18 de novembro de 2025


Micheli Ulian Silva Camargo
Secretária Municipal de Educação

Rua Boa Vista, 323 – CEP 17190-005 – Reginópolis – SP
e-mail: educacao@reginopolis.sp.gov.br



DIÁRIO OFICIAL

MUNICÍPIO DE REGINÓPOLIS

Conforme Lei Municipal nº 2.424, de 19 de dezembro de 2017

Terça-feira, 18 de novembro de 2025

Ano VIII | Edição nº 1489

Página 35 de 35

Licitações e Contratos

Aditivos / Aditamentos / Supressões

EXTRATO

Pregão Presencial nº 032/2021.

Processo Administrativo nº 115/2021.

Contrato Administrativo nº 045/2021.

Partes: **Prefeitura Municipal de Reginópolis e GESTÃO AMBIENTAL LTDA. EIRELI - CNPJ: 02.456.361/0001-72.**

Objeto: ADITAMENTO CONTRATUAL PARA A PRESTAÇÃO DE SERVIÇOS DE COLETA, TRANSPORTE, INCINERAÇÃO E DESTINAÇÃO FINAL DE RESÍDUOS SÓLIDOS DOS SERVIÇOS DE SAÚDE DO MUNICÍPIO DE REGINÓPOLIS /SP.

Data da Assinatura: 19/11/2025.

VALOR TOTAL DA LICITAÇÃO: R\$ 35.040,00 (trinta e cinco mil e quarenta reais) anual e R\$ 2.920,00 (dois mil novecentos e vinte reais) mensais para 400kg/mês de resíduos sólidos.

Ratificação

TERMO DE RATIFICAÇÃO DO PROCESSO DE INEXIGIBILIDADE DE LICITAÇÃO Nº 025/2025.

PROCESSO ADMINISTRATIVO Nº 072/2025.

JEFFERSON AUGUSTO RODRIGUES BUAVA, PREFEITO MUNICIPAL DE REGINÓPOLIS, ESTADO DE SÃO PAULO, no uso de suas atribuições legais, considerando informações, pareceres, documentos e despachos contidos no PROCESSO DE ADMINISTRATIVO Nº 072/2025, AUTORIZO a contratação por INEXIGIBILIDADE com a empresa **PECADO CAPITAL EVENTOS LTDA**, pessoa jurídica de direito privado, inscrita no CNPJ nº 13.702.483/0001-18, pela modalidade inexigibilidade de licitação, que trata por objeto: Contratação de apresentação artística (show) da banda **Pecado Capital**, por inexigibilidade de Licitação, para apresentação no dia 31 de dezembro de 2025, durante a Festa de Réveillon do município, conforme especificações do Termo de Referência.

RATIFICO a dispensa de licitação por INEXIGIBILIDADE, nos termos do inciso II, do artigo 74, da Lei n.º 14.133/21.

AUTORIZO, outrossim, a despesa no valor total de R\$ 45.000,00 (quarenta e cinco mil reais), a ser suportada conforme disponibilidade orçamentária informada pela Diretoria de Finanças.

Reginópolis/SP, 18 de novembro de 2025.

JEFFERSON AUGUSTO RODRIGUES BUAVA
PREFEITO MUNICIPAL DE REGINÓPOLIS