DIÁRIO OFICIAL

Órgão Oficial do Município de Lucena-Paraíba

Lucena -Paraíba, segunda-feira, 31 de agosto de 2026 - Ano 2026 -Nº 5116 www.lucena.pb.gov.br

GABINETE DO PREFEITO

RESOLUÇÃO

PREFEITURA MUNICIPAL DE LUCENA

RESOLUÇÃO Nº 01/2026

Institui a Política de Segurança da Informação do Instituto de Previdência Municipal de Lucena – IPML, estabelece normas para proteção das informações institucionais, dos documentos físicos e digitais, dos sistemas informatizados e dos dados pessoais tratados pela Autarquia Previdenciária, e dá outras providências.

A PRESIDENTE DO **INSTITUTO DE PREVIDÊNCIA MUNICIPAL DE LUCENA – IPML**, no uso das atribuições que lhe confere a legislação municipal vigente,

CONSIDERANDO que a informação constitui ativo estratégico para o funcionamento do Regime Próprio de Previdência Social, sendo indispensável à continuidade das atividades administrativas e previdenciárias;

CONSIDERANDO a necessidade de adotar mecanismos capazes de assegurar a confidencialidade, a integridade, a disponibilidade, a autenticidade e a rastreabilidade das informações sob responsabilidade do Instituto;

CONSIDERANDO as disposições da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), bem como os princípios constitucionais que regem a Administração Pública;

CONSIDERANDO as diretrizes estabelecidas pelo Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social – Pró-Gestão RPPS, especialmente aquelas previstas no requisito 3.1.5 do Manual Pró-Gestão RPPS – Versão 4.1;

CONSIDERANDO, por fim, a necessidade de fortalecer a governança institucional, a gestão de riscos e os controles internos relacionados ao tratamento das informações previdenciárias,

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º. Fica instituída a **Política de Segurança da Informação do Instituto de Previdência Municipal de Lucena – IPML**, aplicável a todos os agentes públicos, conselheiros, membros do Comitê de Investimentos, estagiários, prestadores de serviços e demais pessoas que, de qualquer forma, utilizem informações, documentos, sistemas ou recursos tecnológicos pertencentes à Autarquia.

Art. 2º. Esta Política estabelece normas destinadas a prevenir riscos, disciplinar o tratamento das informações institucionais e assegurar a utilização adequada dos recursos tecnológicos, observando a legislação vigente e as boas práticas de governança pública.

Art. 3º. São objetivos desta Política:

I – preservar a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações institucionais;

II – proteger documentos físicos, digitais e bases de dados contra perda, alteração, destruição ou acesso não autorizado;

III – promover o uso seguro dos sistemas informatizados e dos equipamentos tecnológicos;

IV – assegurar o adequado tratamento dos dados pessoais sob responsabilidade do Instituto, em conformidade com a Lei Geral de Proteção de Dados;

V – fortalecer os controles internos relacionados à gestão documental e tecnológica;

VI – reduzir riscos operacionais decorrentes da utilização inadequada das informações;

VII – incentivar a cultura institucional de segurança da informação e proteção de dados.

Art. 4º. As disposições desta Política deverão ser observadas em todas as atividades desenvolvidas pelo Instituto, independentemente do meio utilizado para produção, armazenamento, transmissão ou compartilhamento das informações.

CAPÍTULO II

DO CAMPO DE APLICAÇÃO

Art. 5º. Esta Política aplica-se, no que couber:

I – ao Diretor-Presidente;

II – aos Diretores;

III – aos servidores efetivos;

IV – aos ocupantes de cargos em comissão;

V – aos membros dos Conselhos Deliberativo e Fiscal;

VI – aos integrantes do Comitê de Investimentos;

VII – aos prestadores de serviços;

VIII – aos consultores, assessores e demais terceiros autorizados a acessar informações institucionais.

Art. 6º. Toda pessoa abrangida por esta Política é responsável pela adequada utilização das informações às quais tiver acesso em razão de suas atividades, devendo adotar as medidas necessárias para preservar sua segurança e impedir qualquer forma de uso indevido.

CAPÍTULO III

DOS CONCEITOS BÁSICOS

Art. 7º. Para os fins desta Política, considera-se:

I – **Informação Institucional:** todo dado, documento, registro, processo, imagem, mensagem ou arquivo produzido, recebido, armazenado ou mantido pelo Instituto, independentemente do formato utilizado;

II – **Ativo de Informação:** qualquer recurso físico ou digital que possua valor para a Autarquia, incluindo equipamentos, sistemas, bancos de dados, documentos, infraestrutura tecnológica e serviços de tecnologia da informação;

III – **Segurança da Informação:** conjunto de medidas administrativas, organizacionais e tecnológicas destinadas a proteger as informações contra acessos indevidos, perdas, alterações ou indisponibilidade;

IV – **Dados Pessoais:** informações relacionadas à pessoa natural identificada ou identificável, nos termos da Lei Geral de Proteção de Dados;

V – **Incidente de Segurança:** evento que provoque ou possa provocar comprometimento da confidencialidade, integridade, disponibilidade ou autenticidade das informações institucionais;

VI – **Usuário:** toda pessoa autorizada a utilizar documentos, equipamentos, sistemas ou quaisquer recursos informacionais do Instituto.

CAPÍTULO IV

DOS PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Art. 8º. A Política de Segurança da Informação será orientada pelos seguintes princípios:

I – legalidade;

II – confidencialidade;

III – integridade;

IV – disponibilidade;

V – autenticidade;

VI – rastreabilidade;

VII – transparência, observadas as restrições legais;

VIII – responsabilidade;

IX – prevenção;

X – continuidade dos serviços públicos;

XI – proteção de dados pessoais;

XII – melhoria contínua da gestão e dos controles internos.

Art. 9º. O acesso às informações institucionais deverá observar os princípios da necessidade, da finalidade e do menor privilégio, permitindo que cada usuário utilize apenas as informações indispensáveis ao desempenho de suas atribuições.

Art. 10. Todos os procedimentos relacionados ao tratamento das informações deverão buscar equilíbrio entre segurança, eficiência administrativa, transparência pública e proteção dos direitos dos segurados, assegurando a conformidade com a legislação vigente e com as diretrizes institucionais.

CAPÍTULO V

DA CLASSIFICAÇÃO DAS INFORMAÇÕES

Art. 11. As informações produzidas, recebidas ou mantidas pelo Instituto deverão ser classificadas conforme o grau de sensibilidade e o impacto que sua divulgação possa ocasionar às atividades institucionais, aos segurados ou à Administração Pública.

Art. 12. Para fins desta Política, as informações classificam-se em:

I – Públicas: informações cuja divulgação seja autorizada pela legislação e destinadas ao acesso da sociedade;

II – Internas: informações destinadas exclusivamente ao funcionamento administrativo do Instituto, cujo acesso restringe-se aos usuários autorizados;

III – Restritas: informações que contenham dados administrativos, previdenciários, financeiros ou pessoais cujo acesso deva limitar-se aos responsáveis por sua utilização;

IV – Sigilosas: informações protegidas por disposição legal, decisão administrativa ou natureza do seu conteúdo, cujo acesso dependerá de autorização específica.

Art. 13. Enquadram-se, entre outras, como informações de acesso restrito ou sigiloso:

I – processos de aposentadoria, pensão e demais benefícios previdenciários;

II – prontuários, cadastros e pastas funcionais;

III – documentos contendo dados pessoais ou dados pessoais sensíveis;

IV – relatórios financeiros e bancários;

V – folha de pagamento;

VI – senhas, certificados digitais e credenciais de acesso;

VII – pareceres técnicos ou jurídicos ainda não publicados;

VIII – documentos protegidos por legislação específica.

CAPÍTULO VI

DAS RESPONSABILIDADES

Art. 14. Compete à Diretoria Executiva:

I – assegurar a implementação desta Política;

II – promover a revisão periódica de seus procedimentos;

III – disponibilizar recursos destinados à proteção das informações institucionais;

IV – estimular ações de capacitação e conscientização;

V – adotar providências quando identificadas irregularidades relacionadas à segurança da informação.

Art. 15. São deveres dos servidores, dirigentes, conselheiros, membros do Comitê de Investimentos e demais usuários autorizados:

I – utilizar corretamente os recursos tecnológicos disponibilizados pelo Instituto;

II – preservar o sigilo das informações sob sua responsabilidade;

III – comunicar imediatamente qualquer incidente ou suspeita de violação da segurança;

IV – zelar pelos documentos físicos e eletrônicos;

V – observar integralmente esta Política e demais normas correlatas.

CAPÍTULO VII

DO CONTROLE DE ACESSO ÀS INFORMAÇÕES

Art. 16. O acesso aos documentos, sistemas informatizados e bases de dados será concedido exclusivamente aos usuários que necessitem das informações para o desempenho de suas atribuições funcionais.

Art. 17. Os perfis de acesso deverão observar os princípios da necessidade, da segregação de funções e do menor privilégio, sendo vedada a concessão de permissões incompatíveis com as atividades exercidas.

Art. 18. Os acessos deverão ser revistos sempre que ocorrer:

I – ingresso de novo servidor ou colaborador;

II – alteração de função;

III – afastamento prolongado;

IV – desligamento;

V – determinação da Diretoria Executiva.

CAPÍTULO VIII

DAS CREDENCIAIS E SENHAS DE ACESSO

Art. 19. Cada usuário receberá credenciais individuais e intransferíveis para acesso aos sistemas institucionais, sendo integralmente responsável pela utilização de sua identificação eletrônica.

Art. 20. As senhas deverão, sempre que possível:

I – possuir nível adequado de complexidade;

II – ser alteradas quando houver suspeita de comprometimento;

III – permanecer sob guarda exclusiva do usuário;

IV – não conter informações pessoais facilmente identificáveis.

Art. 21. É proibido:

I – compartilhar usuários ou senhas;

II – permitir acesso de terceiros utilizando credenciais próprias;

III – registrar senhas em locais de fácil visualização;

IV – utilizar mecanismos que comprometam a segurança dos sistemas.

CAPÍTULO IX

DA UTILIZAÇÃO DOS RECURSOS TECNOLÓGICOS

Art. 22. Os equipamentos de informática, dispositivos móveis, impressoras, scanners e demais recursos tecnológicos disponibilizados pelo Instituto destinam-se prioritariamente ao desenvolvimento das atividades institucionais.

Art. 23. São responsabilidades dos usuários:

I – manter os equipamentos protegidos contra uso indevido;

II – permitir a instalação de atualizações de segurança;

III – bloquear a estação de trabalho quando houver afastamento temporário;

IV – comunicar falhas, defeitos ou comportamentos suspeitos dos equipamentos.

Art. 24. É vedado:

I – instalar softwares sem autorização;

II – alterar configurações de segurança;

III – utilizar programas sem licenciamento quando exigido;

IV – conectar equipamentos particulares que possam comprometer a rede institucional;

V – retirar equipamentos das dependências do Instituto sem autorização.

CAPÍTULO X

DO USO DA INTERNET E DO CORREIO ELETRÔNICO

Art. 25. O acesso à internet disponibilizado pelo Instituto deverá priorizar atividades relacionadas à gestão previdenciária, administrativa e institucional.

Art. 26. O correio eletrônico institucional constitui meio oficial de comunicação administrativa e deverá ser utilizado com linguagem adequada e observância do sigilo das informações.

Art. 27. É vedado:

I – encaminhar documentos institucionais para contas particulares sem autorização;

II – acessar conteúdos que comprometam a segurança da rede;

III – abrir mensagens ou anexos de origem desconhecida;

IV – utilizar o e-mail institucional para finalidades incompatíveis com o interesse público.

CAPÍTULO XI

DA PRESERVAÇÃO DOS DOCUMENTOS E DAS CÓPIAS DE SEGURANÇA

Art. 28. Os documentos físicos e digitais produzidos pelo Instituto deverão permanecer organizados, protegidos e armazenados em ambiente apropriado, garantindo sua integridade, disponibilidade e autenticidade.

Art. 29. Sempre que tecnicamente viável, deverão ser realizadas cópias periódicas de segurança (backup) dos arquivos institucionais, observando procedimentos que permitam sua recuperação em caso de falhas ou incidentes.

Art. 30. Os arquivos considerados essenciais à continuidade das atividades do Instituto deverão possuir mecanismos adicionais de proteção e armazenamento seguro.

CAPÍTULO XII

DA POLÍTICA DE MESA LIMPA E TELA PROTEGIDA

Art. 31. Os documentos contendo informações restritas deverão permanecer guardados em armários, arquivos ou gavetas apropriadas sempre que não estiverem sendo utilizados.

Art. 32. Ao afastar-se da estação de trabalho, o usuário deverá bloquear o computador ou encerrar sua sessão de acesso.

Art. 33. Ao final do expediente deverão ser adotadas, sempre que cabíveis, as seguintes providências:

I – recolhimento dos documentos físicos;

II – guarda adequada dos processos administrativos e previdenciários;

III – desligamento dos equipamentos;

IV – armazenamento seguro das mídias removíveis utilizadas.

CAPÍTULO XIII

DA PROTEÇÃO DOS DOCUMENTOS E DOS DADOS PESSOAIS

Art. 34. Os processos administrativos, previdenciários, pastas funcionais e demais documentos institucionais deverão permanecer organizados e protegidos contra perda, extravio, alteração, destruição ou acesso indevido.

Art. 35. O tratamento de dados pessoais observará integralmente os princípios estabelecidos pela Lei Geral de Proteção de Dados – LGPD, sendo permitido apenas para finalidades institucionais legítimas.

Art. 36. É vedado:

I – fornecer dados pessoais sem respaldo legal;

II – manter cópias particulares de documentos institucionais;

III – divulgar informações cadastrais de segurados ou servidores sem autorização;

IV – utilizar dados pessoais para finalidade diversa daquela autorizada.

CAPÍTULO XIV

DO ATENDIMENTO AOS SEGURADOS E DO COMPARTILHAMENTO DAS INFORMAÇÕES

Art. 37. O atendimento presencial, telefônico ou eletrônico deverá assegurar a privacidade dos segurados, evitando exposição desnecessária de documentos e informações pessoais.

Art. 38. Antes do fornecimento de qualquer informação deverá ser confirmada a identidade do interessado ou de seu representante legal.

Art. 39. O compartilhamento de documentos observará os princípios da necessidade, finalidade e proporcionalidade, limitando-se às informações indispensáveis para cada situação.

Art. 40. A utilização de aplicativos de mensagens instantâneas para envio de documentos institucionais somente será admitida quando necessária ao interesse da Administração e desde que adotadas medidas destinadas à proteção das informações, sendo vedado o envio de folhas de pagamento completas, senhas, documentos sigilosos ou dados pessoais sensíveis sem autorização expressa da Diretoria Executiva.

CAPÍTULO XV

DA GESTÃO DOS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 41. Considera-se incidente de segurança toda ocorrência, acidental ou intencional, capaz de comprometer a confidencialidade, a integridade, a disponibilidade ou a autenticidade das informações sob responsabilidade do Instituto.

Art. 42. Constituem exemplos de incidentes de segurança, entre outros:

I – acesso não autorizado a documentos ou sistemas;

II – perda, extravio ou furto de processos e equipamentos;

III – divulgação indevida de informações institucionais;

IV – vazamento de dados pessoais;

V – utilização inadequada de credenciais de acesso;

VI – infecção por programas maliciosos;

VII – exclusão ou alteração não autorizada de arquivos;

VIII – indisponibilidade dos sistemas informatizados;

IX – envio equivocado de documentos a destinatário não autorizado.

Art. 43. Todo usuário que identificar situação que possa representar risco à segurança das informações deverá comunicar imediatamente o fato à Diretoria Executiva, informando, sempre que possível, a descrição da ocorrência, os documentos ou sistemas envolvidos e as providências já adotadas.

Art. 44. Recebida a comunicação, caberá à Diretoria Executiva:

I – avaliar os impactos do incidente;

II – adotar medidas destinadas à contenção dos danos;

III – preservar evidências quando necessário;

IV – promover ações corretivas e preventivas;

V – acompanhar a recuperação das informações eventualmente afetadas.

CAPÍTULO XVI

DA CONTINUIDADE DOS SERVIÇOS

Art. 45. O Instituto adotará medidas destinadas a preservar a continuidade das atividades previdenciárias e administrativas diante de situações que possam comprometer o funcionamento normal de seus serviços.

Art. 46. Sempre que possível deverão ser mantidos procedimentos que permitam:

I – recuperação de documentos e arquivos;

II – restabelecimento dos sistemas essenciais;

III – continuidade do atendimento aos segurados;

IV – preservação das informações consideradas críticas para a Administração.

CAPÍTULO XVII

DA CAPACITAÇÃO E DA CONSCIENTIZAÇÃO

Art. 47. O Instituto promoverá ações periódicas de orientação sobre Segurança da Informação, proteção de dados pessoais, utilização adequada dos recursos tecnológicos e prevenção de incidentes.

Art. 48. As ações poderão compreender:

I – cursos presenciais;

II – capacitações à distância;

III – palestras;

IV – oficinas;

V – campanhas internas de conscientização;

VI – divulgação de materiais educativos.

Art. 49. Sempre que houver alterações relevantes na legislação, nos sistemas utilizados ou nesta Política, os usuários deverão ser orientados quanto às novas diretrizes adotadas.

CAPÍTULO XVIII

DO ACOMPANHAMENTO E DA VERIFICAÇÃO DO CUMPRIMENTO

Art. 50. Compete à Diretoria Executiva acompanhar a execução desta Política, promovendo avaliações periódicas sobre sua efetividade.

Art. 51. As verificações poderão abranger, entre outros aspectos:

I – utilização dos sistemas informatizados;

II – controle de acesso às informações;

III – armazenamento dos documentos físicos e digitais;

IV – cumprimento das regras estabelecidas nesta Política;

V – adoção das medidas de proteção previstas.

Art. 52. As atividades de acompanhamento terão caráter prioritariamente preventivo e educativo, sem prejuízo da adoção das providências administrativas cabíveis quando constatadas irregularidades.

CAPÍTULO XIX

DAS RESPONSABILIDADES E DAS MEDIDAS ADMINISTRATIVAS

Art. 53. O descumprimento das disposições desta Política sujeitará o responsável às medidas administrativas previstas na

legislação aplicável, sem prejuízo das responsabilidades civil e penal.

Art. 54. Constituem, entre outras, condutas incompatíveis com esta Política:

I – divulgação não autorizada de informações institucionais;

II – compartilhamento de dados pessoais em desacordo com a legislação;

III – utilização de senha ou credencial pertencente a outro usuário;

IV – instalação de programas sem autorização;

V – retirada indevida de documentos;

VI – alteração, destruição ou ocultação de informações institucionais;

VII – qualquer prática que comprometa a segurança das informações do Instituto.

Art. 55. Na apuração de eventual descumprimento serão assegurados o contraditório, a ampla defesa e o devido processo legal.

CAPÍTULO XX

DA ATUALIZAÇÃO DA POLÍTICA

Art. 56. Esta Política deverá ser revisada sempre que:

I – houver alteração da legislação aplicável;

II – ocorrerem mudanças relevantes na estrutura administrativa ou tecnológica do Instituto;

III – forem identificadas vulnerabilidades que recomendem aperfeiçoamento dos controles;

IV – houver necessidade de adequação às atualizações do Programa Pró-Gestão RPPS.

CAPÍTULO XXI

DAS DISPOSIÇÕES FINAIS

Art. 57. Todos os usuários abrangidos por esta Política deverão firmar Termo de Ciência e Responsabilidade, comprometendo-se a observar suas disposições.

Art. 58. A presente Política permanecerá disponível para consulta de servidores, dirigentes, conselheiros, membros do Comitê de Investimentos, estagiários, prestadores de serviços e demais usuários autorizados.

Art. 59. Os casos omissos serão resolvidos pela Diretoria Executiva do Instituto de Previdência Municipal de Lucena – IPML, observadas as normas legais vigentes.

Art. 60. Esta Resolução entra em vigor na data de sua publicação, revogadas as disposições em contrário.

Lucena/PB, 31 de Agosto de 2026.

Thais Emília Diniz Mendes de Araújo Costa
Diretora-Presidente
Instituto de Previdência Municipal de Lucena – IPML

ANEXO I

TERMO DE CIÊNCIA E RESPONSABILIDADE

Eu, _____, ocupante do cargo/função de _____, declaro que recebi, li e compreendi integralmente a **Política de Segurança da Informação do Instituto de Previdência Municipal de Lucena – IPML**.

Comprometo-me a cumprir todas as normas nela estabelecidas, zelando pela confidencialidade, integridade, disponibilidade e proteção das informações, documentos, sistemas e dados pessoais aos quais tiver acesso em razão de minhas atribuições.

Declaro, ainda, estar ciente de que o descumprimento desta Política poderá ensejar a adoção das medidas administrativas, civis e penais cabíveis, na forma da legislação vigente.

Lucena/PB, ____ de _____ de _____.

Nome:

_____

Cargo/Função:

_____

Assinatura:

_____

GABINETE DO PREFEITO

PORTARIA

PREFEITURA MUNICIPAL DE LUCENA

PORTARIA IPML Nº 011/2026

Designa servidor para atuar como responsável pelo acompanhamento e execução da Política de Segurança da Informação do Instituto de Previdência Municipal de Lucena – IPML, e dá outras providências.

A **DIRETORA-PRESIDENTE DO INSTITUTO DE PREVIDÊNCIA MUNICIPAL DE LUCENA – IPML**, no uso das atribuições que lhe são conferidas pela Lei Municipal nº 1.049/2021 e demais disposições legais aplicáveis,

CONSIDERANDO a necessidade de assegurar a proteção das informações, documentos, sistemas, equipamentos e dados pessoais utilizados no âmbito do Instituto de Previdência Municipal de Lucena – IPML;

CONSIDERANDO a instituição da **Política de Segurança da Informação do Instituto de Previdência Municipal de Lucena – IPML**, destinada a estabelecer diretrizes e procedimentos para a proteção das informações institucionais, dos documentos físicos e digitais, dos sistemas informatizados e dos dados pessoais tratados pela Autarquia;

CONSIDERANDO a necessidade de definir responsabilidades para o acompanhamento e a efetiva aplicação das medidas previstas na Política de Segurança da Informação;

CONSIDERANDO as disposições da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais – LGPD, especialmente quanto à necessidade de adoção de medidas de segurança aptas a proteger os dados pessoais tratados pela Administração Pública;

CONSIDERANDO as diretrizes do Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social – **Pró-**

Gestão RPPS, especialmente aquelas relacionadas à Política de Segurança da Informação;

RESOLVE:

Art. 1º - DESIGNAR o servidor **RODRIGO LIMA NERES**, ocupante do cargo de Assistente Administrativo, matrícula nº 1053, para atuar como responsável pelo acompanhamento e execução das diretrizes e procedimentos estabelecidos na Política de Segurança da Informação do Instituto de Previdência Municipal de Lucena – IPML.

Art. 2º - Compete ao servidor designado, no âmbito de suas atribuições e sob a orientação da Diretoria Executiva do IPML:

I – acompanhar o cumprimento das disposições estabelecidas na Política de Segurança da Informação;

II – auxiliar na implementação e execução dos procedimentos de segurança da informação definidos pelo Instituto;

III – acompanhar a aplicação das medidas de proteção dos documentos físicos e digitais, sistemas informatizados, equipamentos e demais ativos de informação do IPML;

IV – acompanhar os procedimentos relacionados ao controle de acesso aos documentos, sistemas, equipamentos e informações institucionais;

V – acompanhar a realização e a adequada guarda das cópias de segurança dos arquivos e documentos institucionais, quando aplicável;

VI – receber e encaminhar à Diretoria Executiva as comunicações relativas a incidentes ou suspeitas de incidentes de segurança da informação;

VII – auxiliar na adoção das medidas necessárias à contenção, correção e prevenção de incidentes de segurança da informação;

VIII – colaborar com as ações de orientação, capacitação e conscientização dos servidores, conselheiros, membros do Comitê de Investimentos, prestadores de serviços e demais usuários abrangidos pela Política de Segurança da Informação;

IX – comunicar à Diretoria Executiva eventuais situações de descumprimento, vulnerabilidades ou riscos identificados no âmbito da segurança da informação; e

X – desempenhar outras atividades relacionadas ao acompanhamento e à execução da Política de Segurança da Informação que lhe sejam atribuídas pela Diretoria Executiva.

Art. 3º - O servidor designado deverá atuar de forma integrada com a Diretoria Executiva, não lhe cabendo, isoladamente, a responsabilidade institucional pela Segurança da Informação, pela proteção de dados pessoais ou pela adoção de medidas administrativas que dependam de decisão da Presidência.

Parágrafo único. A responsabilidade pela implementação, supervisão e aprovação das medidas institucionais relacionadas à Política de Segurança da Informação permanece sob responsabilidade da **Diretoria Executiva do IPML**, na forma estabelecida na própria Política.

Art. 4º - O servidor designado deverá observar, no desempenho de suas atribuições, os princípios da confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, prevenção, responsabilidade e proteção dos dados pessoais, bem como as demais disposições estabelecidas na Política de Segurança da Informação do IPML e na legislação vigente.

Art. 5º - O servidor designado deverá comunicar imediatamente à Diretoria Executiva qualquer incidente, suspeita de violação, perda, extravio, acesso não autorizado, divulgação indevida ou outra ocorrência que possa comprometer a segurança das informações institucionais ou dos dados pessoais tratados pelo IPML.

Art. 6º - A presente designação não afasta a responsabilidade individual de todos os servidores, dirigentes, conselheiros, membros do Comitê de Investimentos, prestadores de serviços e demais usuários autorizados pelo cumprimento das disposições da Política de Segurança da Informação, conforme previsto na respectiva Política.

Art. 7º - A presente Portaria deverá permanecer disponível para consulta dos servidores e demais interessados, juntamente com a Política de Segurança

da Informação do IPML, constituindo-se como documento de formalização da responsabilidade pelo acompanhamento e execução das ações de segurança da informação no âmbito da Autarquia.

Art. 8º - Os casos omissos serão resolvidos pela Diretoria Executiva do Instituto de Previdência Municipal de Lucena – IPML, observadas as disposições legais e regulamentares aplicáveis.

Art. 9º - Esta Portaria entra em vigor na data de sua publicação.

Lucena/PB, 31 de agosto de 2026.

THAÍS EMÍLIA DINIZ MENDES DE ARAÚJO COSTA
Diretora-Presidente
Instituto de Previdência Municipal de Lucena – IPML