PSI — POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

FUNDO DE PREVIDÊNCIA DOS SERVIDORES MUNICIPAIS DE MANDAGUAÇU

Confidencialidade • Integridade • Disponibilidade • Autenticidade

MANDAGUAÇU PARANÁ

02

INTRODUÇÃO

Apresentação

A **Política de Segurança da Informação (PSI)** do Fundo de Previdência dos Servidores Municipais de Mandaguaçu estabelece as diretrizes, responsabilidades e procedimentos destinados à proteção das informações produzidas, recebidas, armazenadas, processadas e transmitidas pela Autarquia Previdenciária.

Princípios basilares

A informação é considerada ativo estratégico e deve ser protegida contra acesso indevido, modificação não autorizada e indisponibilidade indevida, observando-se os princípios da **confidencialidade, integridade, disponibilidade e autenticidade**.

Aplicação

Esta Política aplica-se a todos os servidores efetivos, comissionados, estagiários, prestadores de serviços, conselheiros, membros do Comitê de Investimentos, fornecedores e terceiros que tenham acesso às informações ou aos recursos tecnológicos do Fundo de Previdência.

Conformidade legal e Pró-Gestão RPPS

A PSI está alinhada à **Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD)**, às normas da ABNT aplicáveis e às exigências do Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social — **Pró-Gestão RPPS**, fortalecendo a governança, a transparência e a confiabilidade dos processos institucionais.

03

FUNDAMENTOS

Os Quatro Pilares

São princípios basilares da Política de Segurança da Informação:

Confidencialidade

Proteção e garantia de que determinadas informações só são disponíveis a pessoas autorizadas.

Integridade

Garantia da exatidão das informações e dos métodos de processamento.

Disponibilidade

Garantia de que os usuários autorizados e os interessados tenham acesso às informações.

Autenticidade

Assegurar que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

04

CAPÍTULO I

Cap. I — Disposições Gerais

Art. 1º Fica instituída a Política de Segurança da Informação – PSI do Fundo de Previdência dos Servidores Municipais de Mandaguaçu, com a finalidade de estabelecer diretrizes, responsabilidades e procedimentos destinados à proteção das informações produzidas, recebidas, armazenadas, processadas e transmitidas pela Autarquia Previdenciária.

Art. 2º A presente Política aplica-se a todos os servidores efetivos, comissionados, estagiários, prestadores de serviços, conselheiros, membros do Comitê de Investimentos, fornecedores e terceiros que tenham acesso às informações ou aos recursos tecnológicos do Fundo de Previdência.

Art. 3º A informação, considerada ativo estratégico de valor para o Fundo de Previdência, deve ser adequadamente protegida contra acesso indevido, modificação não autorizada e indisponibilidade indevida.

Art. 4º Para fins desta Política considera-se:

I **Informação:** qualquer dado ou conjunto de dados produzidos ou custodiados pelo Fundo de Previdência;

II **Ativo de Informação:** informações, sistemas, equipamentos, documentos físicos ou digitais utilizados pelo Fundo de Previdência;

III **Incidente de Segurança:** evento que comprometa ou possa comprometer a segurança da informação;

IV **Usuário:** qualquer pessoa autorizada a acessar os recursos informacionais da Autarquia;

V **Dados Pessoais:** informações relacionadas à pessoa natural identificada ou identificável, nos termos da LGPD.

05

CAPÍTULO II

Cap. II — Dos Princípios

Art. 5º São princípios basilares da Política de Segurança da Informação:

I **Confidencialidade:** proteção e garantia de que determinadas informações só são disponíveis a pessoas autorizadas;

II **Integridade:** garantia da exatidão das informações e dos métodos de processamento;

III **Disponibilidade:** garantia de que os usuários autorizados e os interessados tenham acesso às informações;

IV **Autenticidade:** assegurar que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

06

CAPÍTULO III

Cap. III — Dos Objetivos

Art. 6º São objetivos norteadores da Política de Segurança da Informação:

I Estabelecer critérios para o uso adequado dos recursos tecnológicos e dos sistemas de informação da Autarquia;

II Proteger os dados pessoais de segurados, aposentados, pensionistas, dependentes, servidores e prestadores de serviços, em conformidade com a LGPD;

III Reduzir riscos relacionados a perdas, vazamentos, acessos não autorizados, fraudes, indisponibilidade de sistemas e demais incidentes de segurança;

IV Garantir a continuidade das atividades essenciais do Fundo de Previdência mediante backup, recuperação de dados e gestão de incidentes;

V Assegurar o cumprimento das exigências legais, normativas e regulatórias aplicáveis aos RPPS;

VI Fortalecer a governança, a transparência e a confiabilidade dos processos administrativos, financeiros e previdenciários;

VII Estabelecer mecanismos de monitoramento, auditoria e controle que permitam identificar vulnerabilidades e corrigir falhas;

VIII Implementar mecanismos de gestão de riscos de segurança da informação;

IX Fortalecer as práticas de governança institucional e os requisitos de certificação Pró-Gestão RPPS;

X Promover a melhoria contínua dos controles de segurança da informação.

07

CAPÍTULO IV

Cap. IV — Do Controle de Acesso

Art. 7º A autenticação de acesso dos usuários aos sistemas informatizados de gestão do Fundo de Previdência ocorrerá por meio de login e senhas individuais e intransferíveis.

§ 1º Todo usuário deverá possuir credenciais de acesso individuais e intransferíveis, protegidas por senha forte.

§ 2º As senhas deverão ser alteradas periodicamente pelos usuários ou sempre que necessário.

§ 3º Todas as ações executadas por meio do login individual serão de inteira responsabilidade do usuário correspondente.

§ 4º É vedado o compartilhamento de senhas, logins ou outros dispositivos de autenticação.

§ 5º Sempre que tecnicamente viável, os sistemas deverão adotar mecanismos de **autenticação multifator (MFA)** para acesso a informações críticas ou sensíveis.

§ 6º Os acessos concedidos aos usuários deverão ser revisados, no mínimo, uma vez por ano.

Art. 8º As informações produzidas, recebidas, armazenadas ou custodiadas deverão ser classificadas conforme seu grau de sigilo e criticidade nas seguintes categorias:

I **Públicas:** passíveis de divulgação sem restrições legais;

II **Uso Interno:** destinadas exclusivamente ao ambiente institucional;

III **Restritas:** acesso limitado a usuários autorizados;

IV **Confidenciais:** cujo acesso indevido possa causar prejuízos à Autarquia, aos segurados ou a terceiros.

O acesso observará o **princípio do menor privilégio**, sendo concedido apenas aos usuários que necessitem das informações para o desempenho de suas funções.

08

CAPÍTULO V

Cap. V — Correio Eletrônico e Internet

Art. 9º Os recursos de internet, correio eletrônico corporativo, sistemas informatizados, plataformas digitais e quaisquer outros meios tecnológicos deverão ser utilizados exclusivamente para o desempenho das atividades institucionais.

Art. 10 A ferramenta de correio eletrônico corporativo constitui meio de comunicação oficial, a ser utilizada com nome RPPS/setor seguido do domínio <mandaguacu.pr.gov.br>. É vedado o uso de contas particulares de correio eletrônico para fins institucionais.

Art. 11 É vedado o uso inadequado dos recursos tecnológicos, considerando-se abuso qualquer utilização que:

I Comprometa o desempenho das atividades funcionais durante o expediente;

II Coloque em risco a segurança das informações e dos sistemas institucionais;

III Prejudique a imagem, a credibilidade ou a reputação do Fundo de Previdência;

IV Viole a legislação vigente, os princípios da Administração Pública ou as normas internas;

V Promova atividades particulares incompatíveis com o exercício das funções públicas.

Art. 12 É permitida a utilização de aplicativos de mensagens instantâneas, videoconferência e redes sociais (WhatsApp, Telegram, Microsoft Teams, Google Meet e similares) desde que relacionada às atividades institucionais.

Art. 13 O acesso à internet observará os princípios da legalidade, moralidade, impessoalidade, eficiência, segurança e proteção de dados, bem como as restrições:

I Proibido acessar, armazenar, transmitir ou compartilhar conteúdos ilícitos, ofensivos, discriminatórios, pornográficos ou incompatíveis com as atividades institucionais;

II Proibido acessar sites de apostas, jogos de azar, cassinos virtuais ou páginas que representem risco à rede corporativa;

III Proibido o uso de ferramentas P2P, torrents ou similares sem autorização expressa;

IV Proibida a instalação ou utilização de softwares, aplicativos ou extensões não autorizados;

V Proibido realizar downloads de arquivos para fins particulares que possam comprometer a rede ou os sistemas institucionais;

VI Proibido utilizar os recursos para atividades comerciais particulares, propaganda político-partidária ou finalidade estranha ao interesse público.

Art. 14 O correio eletrônico corporativo constitui ferramenta oficial de comunicação institucional, devendo ser utilizado com responsabilidade, ética, profissionalismo e observância às normas de segurança da informação e proteção de dados pessoais.

09

CAPÍTULO VI

Cap. VI — Procedimentos de Backup

Art. 15 O Fundo de Previdência manterá procedimentos de backup que garantam a integridade, disponibilidade e recuperação tempestiva dos dados, em conformidade com a LGPD.

§ 1º Os backups serão realizados de forma automatizada, com periodicidade definida por política interna, preferencialmente fora do horário comercial.

§ 2º As cópias de segurança serão armazenadas em locais seguros, com proteção contra incêndio, umidade, acesso não autorizado e falhas de equipamento, em ambientes distintos do local de produção.

§ 3º Os procedimentos de backup deverão prever:

I A integridade e o versionamento dos dados copiados;

II A identificação clara das mídias e arquivos gerados;

III A guarda em local com controle de acesso físico, conforme normas técnicas da ABNT;

IV A realização de testes periódicos de restauração (restore), com registros documentais;

V A confidencialidade dos dados pessoais nos backups, com criptografia e acesso restrito.

§ 4º Compete à área de Tecnologia da Informação manter inventário das mídias, definir prazos de retenção, promover substituição periódica das mídias e controlar acessos às cópias.

§ 5º Em caso de falha no backup ou restauração, o responsável técnico realizará nova execução, priorizando sistemas críticos e comunicando o incidente.

§ 6º A inobservância das normas de backup configura infração grave e poderá acarretar responsabilização administrativa, civil e/ou penal.

10

CAPÍTULO VII

Cap. VII — Gestão de Incidentes

Art. 16 Todo incidente de segurança da informação deverá ser comunicado imediatamente ao responsável pela Gestão de Segurança da Informação.

§ 1º Consideram-se incidentes de segurança:

I Acesso não autorizado a sistemas ou informações;

II Perda, extravio ou vazamento de dados;

III Indisponibilidade de sistemas críticos;

IV Infecção por vírus, ransomware ou outros códigos maliciosos;

V Qualquer evento que comprometa a confidencialidade, integridade, disponibilidade ou autenticidade das informações.

§ 2º Os incidentes deverão ser registrados, analisados, tratados e documentados, com adoção de medidas corretivas e preventivas.

§ 3º Nos casos envolvendo dados pessoais, observar-se-ão as disposições da LGPD, inclusive quanto à comunicação às autoridades competentes.

11

CAPÍTULO VIII

Cap. VIII — Capacitação e Conscientização

Art. 17 Todos os servidores, conselheiros, membros do Comitê de Investimentos, estagiários e prestadores de serviços com acesso às informações institucionais deverão participar de ações de capacitação e conscientização em segurança da informação e proteção de dados.

§ 1º As capacitações ocorrerão, no mínimo, uma vez ao ano.

§ 2º A participação será registrada e arquivada para controle interno, auditorias e certificações institucionais.

12

CAPÍTULO IX

Cap. IX — Gestão de Riscos

Art. 18 O Fundo de Previdência deverá identificar, avaliar, tratar e monitorar periodicamente os riscos relacionados à segurança da informação.

§ 1º A gestão de riscos deverá contemplar:

I Identificação dos ativos de informação;

II Identificação de vulnerabilidades e ameaças;

III Avaliação dos impactos potenciais;

IV Definição de medidas mitigadoras;

V Monitoramento contínuo dos riscos identificados.

§ 2º O processo de gestão de riscos será revisado anualmente ou sempre que ocorrer alteração relevante nos sistemas, processos ou legislação aplicável.

13

CAPÍTULO X

Cap. X — Privacidade da Informação

Art. 19 O Fundo de Previdência assegura o respeito à privacidade dos dados pessoais e sensíveis sob sua guarda, em conformidade com a Lei nº 13.709/2018 — LGPD.

§ 1º A coleta, tratamento, armazenamento e compartilhamento de dados pessoais devem observar:

I A finalidade específica e legítima;

II A necessidade mínima dos dados para atingir a finalidade proposta;

III O livre acesso dos titulares às informações que lhes digam respeito;

IV A qualidade e exatidão dos dados armazenados;

V A transparência no tratamento, respeitados os segredos institucionais e comerciais;

VI A segurança dos dados contra acessos não autorizados e situações acidentais ou ilícitas.

§ 2º O acesso será restrito a pessoas autorizadas e capacitadas, com registro formal de autorização.

§ 3º Toda informação tratada é considerada patrimônio institucional e deverá ser protegida, inclusive após o término do vínculo do servidor ou colaborador.

§ 4º O compartilhamento de dados pessoais com terceiros exige autorização da Diretoria Executiva ou base legal definida pela LGPD, precedido de avaliação de risco e instrumentos contratuais com cláusulas específicas de proteção de dados.

14

CAPÍTULO XI

Cap. XI — Monitoramento e Auditoria

Art. 20 O Fundo de Previdência poderá adotar mecanismos de monitoramento e auditoria em seus ambientes físicos e digitais, para garantir o cumprimento desta Política, assegurar a integridade dos ativos, prevenir incidentes e promover a responsabilização de infratores.

§ 1º Os acessos a redes, sistemas, e-mails, aplicativos, dispositivos móveis e recursos em nuvem poderão ser monitorados, registrados e auditados conforme critérios técnicos definidos pela TI e validados pela Comissão.

§ 2º O monitoramento observará os princípios da legalidade, proporcionalidade, necessidade, finalidade e transparência, respeitando a privacidade individual conforme a LGPD.

§ 3º A auditoria técnica de sistemas, equipamentos, ambientes, acessos e processos poderá ser realizada:

I Periodicamente, conforme plano anual de auditoria;

II Extraordinariamente, em caso de incidentes, falhas, denúncias ou suspeitas de violação;

III Por demanda da Controladoria Interna, da Comissão ou da Diretoria Executiva;

IV Por exigência de órgãos de controle, fiscalização ou auditoria externa.

§ 4º Os relatórios e logs deverão ser armazenados em ambiente seguro, com controle de integridade e acesso restrito, respeitando prazos legais e critérios de classificação e temporalidade.

§ 5º Evidências de uso indevido, falhas ou violações deverão ser formalmente registradas e encaminhadas às instâncias competentes, podendo ensejar processo administrativo disciplinar e comunicação às autoridades.

§ 6º Poderão ser utilizados sistemas de correlação de eventos, inteligência artificial ou soluções automatizadas de análise comportamental, desde que observadas as salvaguardas legais de proteção à privacidade.

Parágrafo único. As atividades de monitoramento e auditoria serão detalhadas em norma interna complementar, com plano formal, auditável e registros rastreáveis, preservando o equilíbrio entre o controle institucional e os direitos individuais.

15

CAPÍTULO XII

Cap. XII — Infrações e Penalidades

Art. 21 O descumprimento desta Política sujeitará os responsáveis às sanções previstas em normativos internos, na legislação administrativa aplicável e, especialmente, na Lei nº 13.709/2018 — LGPD, observados o contraditório e a ampla defesa.

§ 1º As infrações serão analisadas considerando natureza, gravidade, impacto institucional, prejuízos a titulares de dados e reincidência, podendo ser classificadas como:

I **Leves:** condutas que contrariem diretrizes da PSI sem prejuízos identificáveis;

II **Médias:** ações ou omissões que comprometam a segurança da informação de forma moderada;

III **Graves:** condutas dolosas ou que resultem em prejuízo à integridade, confidencialidade ou disponibilidade de dados, ou que caracterizem violação à LGPD.

§ 2º As penalidades aplicáveis incluem:

I Advertência verbal ou escrita;

II Suspensão de acesso a sistemas e recursos informacionais;

III Responsabilização funcional, contratual, civil e/ou penal;

IV Demissão por justa causa, nos casos previstos em lei;

V Indenização por danos causados a terceiros ou à instituição, nos termos da legislação vigente.

§ 3º Nos casos envolvendo tratamento indevido de dados pessoais, serão aplicáveis as sanções dos arts. 52 a 54 da LGPD, incluindo advertência, bloqueio ou eliminação dos dados, comunicação aos titulares afetados e outras medidas legais.

18

CAPÍTULO XIII

Cap. XIII — Disposições Finais

Art. 22 Art. 24 A presente Política de Segurança da Informação deverá ser amplamente divulgada, publicada no sítio eletrônico oficial do Fundo de Previdência e incorporada aos processos de integração de novos servidores e colaboradores.

Art. 25 A Política deverá ser revista periodicamente, no máximo a cada 4 (quatro) anos, ou sempre que houver mudanças relevantes na legislação, nos processos institucionais ou nos sistemas de informação utilizados.

Art. 26 Os casos omissos ou situações não previstas nesta Política serão analisados pelo Comitê de Segurança da Informação, com parecer técnico da área de Tecnologia da Informação, e submetidos à decisão da Diretoria Executiva.

Art. 27 Esta Política entra em vigor na data de sua aprovação e revoga disposições anteriores que lhe sejam contrárias.

Mandaguaçu – Paraná

Fundo de Previdência dos Servidores Municipais de Mandaguaçu
ESTADO DO PARANÁ
CNPJ.: **85.44G.G32/0001-7G**
Rua Bernardino Bogo, 85 – Apto. 01 – Centro – CEP 87160-266
e-mail: *rpps@mandaguacu.pr.gov.br*

FUNDO DE PREVIDÊNCIA
DOS SERVIDORES MUNICIPAIS
DE MANDAGUAÇU

ATA DA REUNIÃO ORDINÁRIA DO CONSELHO DELIBERATIVO DO FUNDO DE PREVIDÊNCIA DOS SERVIDORES DE MANDAGUAÇU

Aos vinte oito dias do mês de junho de dois mil e vinte e seis, na sala de reuniões do Fundo de Previdência, por volta das 14h20, reuniram-se os membros, reuniram-se os membros do Conselho Deliberativo, Sra. Silenita da Silva Welker, Sra. Aline Fabrícia da Silva Martins, Sra. Eliane Ferreira Martins Montovanelli, Sra. Heloisa Vieira Papa e o Sr. José Adirson Gianotto Nascimento juntamente com a servidora Cláudia Caroline Vicentini e o Presidente do Fundo de Previdência, Sr. José Pedro Barbosa Filho. Nessa oportunidade, foram apresentados relatórios detalhados referentes ao mês de maio e ao segundo trimestre de dois mil e vinte e seis, abordando a rentabilidade e os riscos das diversas modalidades de operações realizadas nas aplicações dos recursos do RPPS, bem como a aderência à Política Anual de Investimentos. Em 30/06/2026, o RPPS possuía recursos financeiros na ordem de R$ 68.915.338,29, distribuídos da seguinte forma: CDI: 49,84%; IDKA IPCA 2A: 7,22%; IRF-M: 16,20%; Vértice Médio: 7,60%; IRF-M 1: 5,69%; Crédito Privado: 2,90%; Títulos Públicos: 7,67%; Gestão Livre: 2,87%. Evidenciou-se, de acordo com o relatório, que as aplicações cumpriram o enquadramento previsto na Política de Investimentos vigente. Observou-se que, considerando o comportamento das aplicações, a rentabilidade da carteira foi de +0,90% no mês. A rentabilidade acumulada atingiu +6,53%, enquanto a meta atuarial acumulada prevista para 2026 é de +6,08%. Diante dos resultados apresentados, verificou-se que os investimentos da carteira estão superando a meta atuarial e contribuindo para o aumento do patrimônio do Fundo. Dessa forma, os relatórios foram aprovados por unanimidade. A servidora Claudia realizou a apresentação da Cartilha Previdenciária, elaborada com o objetivo de fortalecer a educação previdenciária e facilitar o acesso dos segurados às principais informações sobre o RPPS de Mandaguaçu. Durante a apresentação, foram destacados os temas abordados na cartilha, como a missão, visão e valores do Fundo, os regimes previdenciários, os segurados e dependentes, bem como a identidade visual da instituição. Também foi informado que serão disponibilizados aos segurados o Código de Ética, a Política de Segurança da Informação e os demais documentos institucionais relacionados às boas práticas de governança e transparência. Após os esclarecimentos, os membros do Conselho manifestaram-se favoravelmente ao material, aprovando sua publicação e divulgação aos segurados. Após os esclarecimentos, os membros manifestaram-se favoravelmente ao material, aprovando sua publicação e divulgação aos segurados. Nada mais havendo a tratar, foi encerrada a reunião, sendo lavrada a presente ata que, após lida e achada conforme, vai assinada por mim e pelos demais membros presentes.

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: A44E-0154-7559-93A6

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

JOSE PEDRO BARBOSA FILHO (CPF 023.XXX.XXX-12) em 04/08/2026 07:09:05 GMT-03:00
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

ELIANE FERREIRA MARTINS MONTOVANELLI (CPF 025.XXX.XXX-66) em 04/08/2026 07:35:38 GMT-03:00
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

JOSÉ ADIRSON GIANOTTO NASCIMENTO (CPF 750.XXX.XXX-44) em 04/08/2026 08:30:11 GMT-03:00
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

HELOISA VIEIRA PAPA (CPF 053.XXX.XXX-38) em 04/08/2026 09:13:57 GMT-03:00
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

ALINE FABRICIA DA SILVA MARTINS (CPF 092.XXX.XXX-88) em 04/08/2026 10:09:02 GMT-03:00
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

CLAUDIA CAROLINE VICENTINI (CPF 077.XXX.XXX-96) em 04/08/2026 13:43:14 GMT-03:00
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

SILENITA DA SILVA WELKER (CPF 175.XXX.XXX-63) em 04/08/2026 15:01:34 GMT-03:00
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://mandaguacu.1doc.com.br/verificacao/A44E-0154-7559-93A6