FUNDAÇÃO DA SEGURIDADE SOCIAL DOS SERVIDORES PÚBLICOS MUNICIPAIS DE SOROCABA
FUNSERV

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

VERSÃO 1.0

Garante a proteção das informações da FUNSERV, assegurando:

- Confidencialidade: acesso apenas por pessoas autorizadas.
- Integridade: dados exatos e sem alterações indevidas.
- Disponibilidade: acesso sempre que necessário.
- Autenticidade: origem e veracidade comprovadas.
- Rastreabilidade: registro de todas as ações.
- Conformidade legal: cumprimento de leis (LGPD, LAI, Pró-Gestão)

ABRIL/2026

CLASSIFICAÇÃO DO DOCUMENTO: **PÚBLICO**

1 Sumário

2 HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
22.04.2026	1.0	Conclusão da primeira versão do relatório	Micael Fidel, Fernando Cunha e Gabriel Schonfelder

3 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

FUNSERV – Fundação da Seguridade Social dos Servidores Públicos Municipais de Sorocaba

---

3.1 PREÂMBULO

A FUNSERV – Fundação da Seguridade Social dos Servidores Públicos Municipais de Sorocaba, instituída em 1º de março de 1993, pela Lei Municipal nº 4168, de 1º de março de 1993, é uma fundação pública municipal dotada de autonomia administrativa, financeira e patrimonial, responsável pela gestão integrada do Regime Próprio de Previdência Social (RPPS) e da assistência à saúde dos servidores públicos municipais ativos, inativos, pensionistas e seus dependentes.

Em razão da natureza de suas atribuições, a FUNSERV trata diariamente volume expressivo de informações sensíveis, incluindo dados pessoais e dados de saúde protegidos por sigilo profissional. A proteção adequada dessas informações é essencial para:

- O cumprimento das obrigações legais e regulatórias (Lei de Acesso à Informação – LAI, Lei Geral de Proteção de Dados – LGPD, normas do Ministério da Previdência);
- A manutenção do **Selo Pró-Gestão RPPS Nível 3**, que exige controles robustos de governança e segurança da informação;
- A preservação da confiança dos segurados e da sociedade;
- A continuidade e a integridade dos serviços prestados.

Esta Política de Segurança da Informação (PSI) estabelece os princípios, diretrizes, responsabilidades e controles fundamentais para garantir a proteção das informações sob a guarda e tratamento da FUNSERV, em conformidade com a legislação aplicável e com as melhores práticas de governança.

3.2 FUNDAMENTAÇÃO LEGAL

A presente Política é instituída com fundamento nas seguintes normas:

- **Constituição Federal, art. 37** – princípios da administração pública (legalidade, impessoalidade, moralidade, publicidade e eficiência);
- **Lei nº 9.717/1998** – dispõe sobre regras gerais para a organização e o funcionamento dos regimes próprios de previdência social dos servidores públicos;
- **Lei nº 10.887/2004** – dispõe sobre a aplicação das disposições da Emenda Constitucional nº 41/2003 aos regimes próprios de previdência social;
- **Portaria MTP nº 1.467/2022** – estabelece diretrizes para o Pró-Gestão RPPS;
- **Portaria MPS nº 185/2015 (Pró-Gestão RPPS)** – define os requisitos de certificação para os RPPS;
- **Manual do Pró-Gestão RPPS – Versão 3.6/2025** – detalha os critérios para obtenção e manutenção da certificação;
- **Lei nº 13.709/2018 (LGPD)** – Lei Geral de Proteção de Dados Pessoais;
- **Lei nº 12.527/2011 (LAI)** – Lei de Acesso à Informação;
- Demais normas aplicáveis à administração pública e aos regimes próprios de previdência social.

3.3 CAPÍTULO I – DISPOSIÇÕES GERAIS

3.3.1 Art. 1º – Finalidade

Esta Política estabelece os princípios, diretrizes, responsabilidades e controles para garantir a proteção das informações da FUNSERV, assegurando:

Pilar	Descrição
Confidencialidade	As informações são acessíveis apenas por pessoas autorizadas, em especial dados pessoais e de saúde.
Integridade	As informações são completas, exatas e não sofrem alterações não autorizadas.

Pilar	Descrição

Disponibilidade	As informações estão acessíveis quando e onde necessárias, com continuidade dos serviços.
Autenticidade	É possível verificar a origem e a veracidade das informações.
Rastreabilidade	Toda ação sobre as informações pode ser auditada, registrando-se quem, quando e o que foi feito.
Conformidade legal	Todas as atividades de tratamento da informação atendem à legislação aplicável.

3.3.2 Art. 2º – Abrangência

Esta Política aplica-se a:

Sujeitos	**Ativos**
Servidores efetivos e comissionados	Sistemas corporativos (previdência e saúde)
Conselheiros (CA, CF, CIP, CIS, CFS)	Equipamentos de TI (computadores, servidores, redes)
Estagiários	Bases de dados e repositórios
Prestadores de serviço (terceirizados, fornecedores)	Documentos físicos e digitais
Demais pessoas que, a qualquer título, tenham acesso a informações da FUNSERV	Infraestrutura de suporte (nuvem, data center)

3.4 CAPÍTULO II – DEFINIÇÕES

3.4.1 Art. 3º – Definições

Para os fins desta Política, consideram-se:

Termo	Definição
Informação	Qualquer dado, físico ou digital, produzido ou custodiado pela FUNSERV.
Incidente de Segurança	Evento confirmado ou suspeito que comprometa ou ameace a confidencialidade, integridade, disponibilidade, autenticidade ou rastreabilidade da informação.
Ativo de Informação	Sistemas, equipamentos, bancos de dados, documentos e infraestrutura que suportam o tratamento das informações.
Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável (ex: nome, CPF, endereço, matrícula).
Dado pessoal sensível	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
Tratamento	Toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação.
Classificação da informação	Processo de definição do nível de proteção necessário a uma informação, conforme seu grau de sensibilidade e impacto institucional.
Controle de acesso	Conjunto de medidas técnicas e administrativas destinadas a garantir que apenas usuários autorizados possam acessar determinadas informações ou sistemas.

3.5 CAPÍTULO III – GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO

3.5.1 Art. 4º – Estrutura de Governança

Fica instituída a Estrutura de Governança da Segurança da Informação, composta pelos seguintes papéis:

Papel	**Atribuições**
Responsável pela Segurança da Informação (RSI)	– Elaborar, revisar e propor atualizações da PSI; – Coordenar a implementação dos controles; – Monitorar riscos e manter a Matriz de Riscos atualizada; – Elaborar o Relatório Anual de Segurança da Informação; – Coordenar a gestão de incidentes; – Manter registros e evidências para auditorias do Pró-Gestão.
Área de Tecnologia da Informação (TI)	– Implementar e manter controles técnicos; – Garantir backups e a continuidade dos serviços; – Gerenciar acessos lógicos (criação, alteração, revogação); – Manter logs e registros de auditoria.
Diretoria Executiva	– Aprovar esta Política e suas atualizações; – Assegurar os recursos orçamentários e humanos necessários; – Garantir o cumprimento institucional da PSI.

3.6 CAPÍTULO IV – GESTÃO DE RISCOS

3.6.1 Art. 5º – Gestão de Riscos em Segurança da Informação

A FUNSERV adotará processo formal, contínuo e documentado de gestão de riscos em segurança da informação, em consonância com os princípios da LGPD e com os requisitos do Pró-Gestão RPPS.

§1º O processo será baseado na identificação, análise, avaliação e tratamento de riscos que possam comprometer a confidencialidade, integridade, disponibilidade e autenticidade das informações institucionais.

§2º A gestão de riscos compreenderá:

Etapa	Descrição
Identificação de ativos críticos	Mapear os sistemas, bases de dados e informações essenciais para a FUNSERV.
Identificação de ameaças e vulnerabilidades	Levantar possíveis eventos que possam comprometer a segurança.
Avaliação de impacto e probabilidade	Classificar cada risco conforme a probabilidade de ocorrência e o impacto potencial.
Definição de controles mitigatórios	Estabelecer medidas preventivas, detectivas e corretivas.
Revisão anual	Atualizar a Matriz de Riscos anualmente ou sempre que houver mudanças significativas.

§3º Os resultados serão formalizados em documento próprio denominado **Matriz de Riscos de Segurança da Informação**, aprovada pela Diretoria Executiva e revisada anualmente.

3.7 CAPÍTULO V – CLASSIFICAÇÃO DA INFORMAÇÃO

3.7.1 Art. 6º – Níveis de Classificação

As informações produzidas, recebidas ou custodiadas pela FUNSERV deverão ser classificadas conforme o grau de sensibilidade e o impacto institucional decorrente de sua divulgação, alteração ou perda, observando-se as seguintes categorias:

Nível	Definição	Exemplos na FUNSERV
Pública	Divulgação permitida ou obrigatória por lei; não acarreta prejuízo institucional, legal ou à privacidade de terceiros.	Relatórios de gestão consolidados, balancetes, editais, informações do Portal da Transparência.
Uso Interno	Destinada exclusivamente ao uso administrativo interno; divulgação indevida não gera impacto relevante.	Memorandos internos, manuais operacionais, procedimentos administrativos.
Restrita	Acesso limitado a servidores autorizados por conter dados pessoais, dados financeiros ou elementos protegidos por lei.	Processos de aposentadoria, cadastros de segurados, guias médicas, autorizações de procedimentos.
Sigilosa	Divulgação indevida pode causar grave dano institucional, jurídico ou pessoal; acesso estritamente controlado.	Chaves criptográficas, política de investimentos não divulgada, bases biométricas, investigações em curso.

§1º A classificação observará critérios de interesse público, impacto institucional, financeiro, reputacional, conformidade legal (especialmente LGPD) e necessidade de acesso para desempenho da função.

§2º Em caso de dúvida quanto à classificação, o servidor deverá adotar o nível mais restritivo e consultar o **Responsável pela Segurança da Informação (RSI).**

§3º O detalhamento das categorias, exemplos e controles aplicáveis encontra-se na **Política de Classificação da Informação (Anexo I)**.

3.8 CAPÍTULO VI – CONTROLE DE ACESSO

3.8.1 Art. 7º – Controle de Acesso Lógico e Físico

O acesso às informações observará o princípio do **menor privilégio** (need-to-know), sendo garantido apenas o necessário ao desempenho das funções.

§1º – Controle de Acesso Lógico

Medida	**Descrição**
Usuário individual e intransferível	Cada servidor possui login único; compartilhamento de credenciais é vedado.
Senha com requisitos mínimos	Mínimo de 8 caracteres, incluindo maiúscula, minúscula, número e caractere especial.
Autenticação multifator (MFA)	Sempre que possível, será exigido um segundo fator (token, biometria).
Revisão periódica de perfis	Os acessos são revisados trimestralmente para garantir alinhamento às funções.
Registro de logs	Todas as tentativas de acesso (sucesso ou falha) são registradas e mantidas por período definido.
Bloqueio automático	Após cinco tentativas inválidas consecutivas, a conta é bloqueada temporariamente.

§2º – Controle de Acesso Físico

Medida	**Descrição**
Restrição às áreas críticas	Salas de servidores, arquivo provisório e outras áreas sensíveis têm acesso controlado.

Medida	**Descrição**
Controle de chaves ou dispositivos eletrônicos	Acesso mediante crachá, biometria ou chave física registrada.
Registro de visitantes	Visitantes e prestadores de serviço são identificados e acompanhados, conforme a criticidade do ambiente.

§3º O detalhamento dos procedimentos encontra-se nos **Manuais de Controle de Acesso Lógico (Anexo II)** e **Físico (Anexo III)**.

3.9 CAPÍTULO VII – USO ACEITÁVEL DOS RECURSOS DE TI

3.9.1 Art. 8º – Uso Aceitável

Os recursos tecnológicos da FUNSERV (computadores, redes, internet, e-mail, sistemas) destinam-se exclusivamente às atividades institucionais.

§1º – **Proibições**

É vedado:

Proibição
Instalar softwares não autorizados (não licenciados ou sem aprovação da TI).
Compartilhar credenciais de acesso.
Utilizar os recursos para fins ilícitos.
Armazenar conteúdos inadequados (arquivos piratas, pornografia, materiais que afrontem a moralidade ou a boa conduta).

§2º O detalhamento das regras de uso encontra-se nos seguintes normativos:

- Anexo IV – Normativo de Uso da Internet
- Anexo V – Normativo de Uso de E-mail
- Anexo VI – Normativo de Uso de Equipamentos de TI

3.10 CAPÍTULO VIII – BACKUP E CONTINUIDADE

3.10.1 Art. 9º – Política de Backup e Plano de Contingência

A FUNSERV manterá política formal de backup e plano de contingência visando garantir a continuidade dos serviços.

Ação	Descrição
Backups periódicos automatizados	Os sistemas críticos têm backup diário, com retenção conforme a Tabela de Temporalidade.
Armazenamento seguro	As cópias de backup são mantidas em local seguro, preferencialmente em nuvem ou em local físico distinto da sede.
Testes de restauração	Periodicamente, são realizados testes de restauração para garantir a recuperação dos dados.
Plano de Recuperação em caso de desastre	Define os procedimentos para restabelecer os serviços essenciais dentro de prazos predefinidos.

§1º O detalhamento encontra-se no **Manual de Backup e Plano de Contingência (Anexo VII)**.

3.11 CAPÍTULO IX – GESTÃO DE INCIDENTES

3.11.1 Art. 10º – Comunicação e Tratamento de Incidentes

Considera-se incidente de segurança da informação qualquer evento confirmado ou suspeito que possa comprometer a confidencialidade, integridade, disponibilidade, autenticidade ou rastreabilidade das informações da FUNSERV.

§1º Todo servidor ou colaborador que identificar ou suspeitar da ocorrência de incidente deverá comunicar imediatamente ao **Responsável pela Segurança da Informação (RSI)** ou à **área de Tecnologia da Informação (TI)**.

§2º O tratamento do incidente compreenderá:

Etapa	Descrição

Registro formal	Data, hora, descrição e fontes do incidente.
Classificação	Quanto à gravidade (SEV-1 a SEV-4).
Contenção	Isolamento de sistemas, bloqueio de acessos, preservação de evidências.
Análise de causa	Identificação da causa raiz.
Erradicação e recuperação	Correção da causa e restauração dos serviços.
Elaboração de relatório	Documentação conclusiva para lições aprendidas.

§3º Quando o incidente envolver dados pessoais e puder acarretar risco ou dano relevante aos titulares, será avaliada a necessidade de comunicação à **Autoridade Nacional de Proteção de Dados (ANPD)** e aos titulares, nos termos da Lei nº 13.709/2018.

§4º O procedimento detalhado está previsto no **Plano de Resposta a Incidentes** (documento autônomo complementar à PSI).

3.12 CAPÍTULO X – PROTEÇÃO DE DADOS PESSOAIS

3.12.1 Art. 11º – Tratamento de Dados Pessoais

O tratamento de dados pessoais observará a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), bem como os princípios da finalidade, adequação, necessidade, segurança, prevenção, não discriminação e responsabilização.

§1º O tratamento de dados pessoais deverá estar vinculado a finalidade legítima, específica e compatível com as atribuições legais e institucionais da FUNSERV, observando-se a respectiva base legal aplicável.

§2º O tratamento de dados pessoais sensíveis será realizado com controles de acesso restritos, medidas técnicas e administrativas reforçadas de segurança e registro de acesso quando aplicável.

§3º A FUNSERV manterá registro das operações de tratamento de dados pessoais realizadas no âmbito institucional, contendo, no mínimo:

Informação

Finalidade do tratamento

Categoria de dados tratados

Agentes envolvidos (controlador, operadores)

Eventuais compartilhamentos realizados

Prazos de retenção

§4º Serão assegurados aos titulares dos dados os direitos previstos na legislação vigente, inclusive:

- Confirmação da existência de tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação, quando cabíveis, observadas as hipóteses legais de retenção obrigatória;
- Portabilidade (quando aplicável);
- Informação sobre compartilhamento com terceiros;
- Revogação de consentimento (quando aplicável).

§5º Incidentes que envolvam dados pessoais serão tratados conforme o procedimento institucional de gestão de incidentes, sendo avaliada a necessidade de comunicação à ANPD e aos titulares.

§6º Quando o tratamento de dados pessoais puder gerar alto risco aos direitos e liberdades dos titulares, será elaborado **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)** , conforme previsto na legislação vigente.

§7º A responsabilidade da FUNSERV quanto à proteção dos dados pessoais restringe-se às informações mantidas sob sua guarda, tratamento ou custódia institucional, inclusive cópias arquivadas para fins legais, administrativos ou de controle.

§8º A utilização, guarda ou eventual divulgação da via regularmente entregue ao titular ou seu representante legal constitui ato de sua exclusiva responsabilidade, não caracterizando incidente de segurança da informação no âmbito institucional, salvo se decorrente de falha comprovada nos procedimentos de entrega ou identificação.

3.13 CAPÍTULO XI – CONSCIENTIZAÇÃO E TREINAMENTO

3.13.1 Art. 12º – Plano de Capacitação

A FUNSERV implementará **Plano Anual de Conscientização e Capacitação em Segurança da Informação e Proteção de Dados Pessoais**, com o objetivo de promover a cultura institucional de segurança, prevenção de incidentes e conformidade legal.

§1º As ações de capacitação abrangem, no mínimo:

Conteúdo
Boas práticas de segurança da informação
Uso adequado de sistemas e recursos tecnológicos
Proteção de dados pessoais e diretrizes da LGPD

Conteúdo
Prevenção e comunicação de incidentes de segurança
Classificação e tratamento adequado das informações

§2º As capacitações serão realizadas periodicamente, podendo ocorrer de forma presencial, remota ou por meio de materiais digitais, cartilhas, comunicados ou campanhas institucionais.

§3º A participação nas ações de capacitação deverá ser registrada em sistema institucional ou outro meio formal de controle, para fins de acompanhamento e auditoria.

§4º Novos servidores, estagiários e colaboradores deverão receber orientação inicial sobre esta Política e suas responsabilidades quanto à segurança da informação.

3.14 CAPÍTULO XII – MONITORAMENTO E AUDITORIA

3.14.1 Art. 13º – Relatório Anual de Gestão

A FUNSERV manterá registros e evidências para fins de auditoria do Pró-Gestão RPPS e demais órgãos de controle.

§1º O RSI irá elaborar o **Relatório Anual de Gestão de Segurança da Informação** contendo:

Item
Indicadores de incidentes (quantidade, tipo, tempo de resposta)
Avaliação de riscos (atualização da Matriz de Riscos)
Ações implementadas no período (com destaque para novos procedimentos)
Recomendações de melhoria

§2º O relatório será submetido à Diretoria Executiva e ao Conselho Administrativo, servindo como base para a tomada de decisão e para a melhoria contínua.

3.15 CAPÍTULO XIII – SANÇÕES

3.15.1 Art. 14º – Responsabilização

O descumprimento das disposições desta Política poderá ensejar responsabilização administrativa, civil e penal, conforme legislação aplicável.

Esfera	**Consequências**
Administrativa	Advertência, suspensão, demissão (para servidores); rescisão contratual (para prestadores de serviço).
Civil	Indenização por danos morais ou materiais, conforme Código Civil e LGPD.
Penal	Responsabilização por crimes contra a administração pública, violação de sigilo funcional, invasão de dispositivo informático, etc., conforme Código Penal e Lei de Abuso de Autoridade.

3.16 CAPÍTULO XIV – DISPOSIÇÕES FINAIS

3.16.1 Art. 15º – Revisão

Esta Política será revisada:

- **Anualmente**, para adequação a mudanças legais, tecnológicas ou organizacionais;
- **Sempre que houver alteração legal relevante** que impacte a segurança da informação ou a proteção de dados;
- **Por determinação da Diretoria Executiva** ou do Conselho Administrativo, em resposta a incidentes ou recomendações de auditoria.

3.16.2 Art. 16º – Vigência

Esta Política entra em vigor na data de sua aprovação pela Diretoria Executiva e homologação pelo Conselho Administrativo, revogadas as disposições anteriores em contrário.

3.16.3 Art. 17º – Anexos

Integram esta Política os seguintes anexos, que detalham procedimentos específicos:

Anexo	Conteúdo
Anexo I	Política de Classificação da Informação
Anexo II	Manual de Controle de Acesso Lógico
Anexo III	Manual de Controle de Acesso Físico
Anexo IV	Normativo de Uso da Internet
Anexo V	Normativo de Uso de E-mail
Anexo VI	Normativo de Uso de Equipamentos de TI
Anexo VII	Manual de Backup e Plano de Contingência
Anexo VIII	Tabela de Temporalidade e Plano de Classificação Documental
Anexo IX	Modelo de Notificação à ANPD

EQUIPE RESPONSÁVEL PELA ELABORAÇÃO

Fernando Cunha Alves (Analista de Sistemas)

Gabriel Augusto Moreira da Silva (Chefe de Seção)

Gabriel Schonfelder Felisberto (Agente de Proteção de Dados)

Giovane de Lucas Haddad (Analista de Sistemas)

Gustavo Gomes Novaes (Chefe da Divisão Administrativa)

Juliano Naoto de Arruda (Técnico de Controle Administrativo)

Leonardo Filipe de Moraes (Técnico de Controle Administrativo)

Micael Fidel Rodrigues Nunes (Chefe de Seção)

SETORES ENVOLVIDOS

Seção de Gestão Documental

Proteção de Dados

Divisão Administrativa Tecnologia da Informação

DIRETORIA EXECUTIVA

FABIO SALUN SILVA
Presidente

EDGAR APARECIDO FERREIRA DA SILVA
Diretor Financeiro

ANA LUCIA BITTENCOURT ROSA
Supervisora Administrativa

MARIA DO SOCORRO SOUZA LIMA
Diretora de Previdência

FUNDAÇÃO DA SEGURIDADE SOCIAL DOS SERVIDORES PÚBLICOS MUNICIPAIS DE SOROCABA – FUNSERV

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: D9EA-7A7F-D6A3-BD5F

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

- FABIO SALUN SILVA (CPF 106.XXX.XXX-35) em 22/04/2026 15:05:17 GMT-03:00
  Papel: Parte
  Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

- EDGAR APARECIDO FERREIRA DA SILVA (CPF 338.XXX.XXX-06) em 22/04/2026 16:59:28 GMT-03:00
  Papel: Parte
  Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

- MARIA DO SOCORRO SOUZA LIMA (CPF 062.XXX.XXX-65) em 23/04/2026 09:48:38 GMT-03:00
  Papel: Parte
  Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

- ANA LUCIA BITTENCOURT ROSA (CPF 152.XXX.XXX-41) em 23/04/2026 11:12:33 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://funservsorocaba.1doc.com.br/verificacao/D9EA-7A7F-D6A3-BD5F

Rodrigo Alcântara

Assinado de forma digital por Rodrigo Alcântara
Dados: 2026.05.05 16:45:23 -03'00'