POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SUPERINTENDENTE EXECUTIVO DO PRESERV

GERALDO BATISTA FILHO

COMISSÃO DO PRÓ-GESTÃO:

BRENDA KAROLLYNE SILVA

ELENI SOARES SANTOS ANDRÉ

HEBERTON DA SILVA TOLENTINO

HERMAK PIRES DE OLIVEIRA

MIRIANE APARECIDA BATISTA

Versão 1.0

Sumário

1. SEGURANÇA DA INFORMAÇÃO

Na esfera da administração pública, a informação constitui um dos bens mais valiosos, essencial para a transparência, a eficiência e a prestação de serviços à sociedade. Um fluxo de informação seguro, confiável e bem gerido é fundamental para a tomada de decisões, o controle social e o cumprimento das finalidades institucionais. Contudo, esse valor, aliado à crescente digitalização e à facilidade de acesso, torna a informação um alvo constante de ameaças — tanto internas quanto externas.

No caso do Instituto de Previdência Social dos Servidores Públicos Municipais – PRESERV, a proteção desses ativos informacionais é imperativa, mesmo quando os dados possuem natureza pública. A má gestão desses riscos pode comprometer a governança, a continuidade dos serviços e a confiança da sociedade na administração pública.

Diante desse cenário, o PRESERV instituiu sua **Política de Segurança da Informação**, como pilar estratégico para salvaguardar seus ativos informacionais e assegurar o alinhamento com os princípios da administração pública: legalidade, impessoalidade, moralidade, publicidade e eficiência.

A Segurança da Informação, nesse contexto, representa um conjunto contínuo de ações voltadas à proteção dos dados sob responsabilidade da autarquia, contribuindo diretamente para o cumprimento de sua missão institucional. Para tanto, a política orienta-se pelos seguintes pilares:

- **Confidencialidade:** assegurar que as informações sejam acessíveis somente às pessoas devidamente autorizadas, respeitando a legislação vigente e os regimes de sigilo aplicáveis;

- **Integridade:** garantir que os dados permaneçam íntegros, protegidos contra alterações não autorizadas, acidentais ou intencionais;

- **Disponibilidade:** assegurar que as informações estejam acessíveis e utilizáveis por usuários autorizados sempre que necessárias ao exercício das funções públicas.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2.1 PROTEÇÃO DA INFORMAÇÃO

Na administração pública, a informação é um ativo estratégico fundamental para o planejamento, a execução e o controle das políticas públicas, bem como para a garantia da transparência, da legalidade e da eficiência na gestão dos recursos públicos. Assim como os demais bens sob responsabilidade do Instituto de Previdência Social dos Servidores Públicos Municipais – PRESERV, a informação deve ser tratada com rigor, responsabilidade e proteção adequada.

A informação pode se apresentar em múltiplos formatos: *sistemas informatizados, diretórios de rede, bancos de dados, documentos impressos, mídias magnéticas ou ópticas, dispositivos eletrônicos, equipamentos portáteis, microfilmes e até mesmo por meio da comunicação oral*. Independentemente de sua forma ou suporte, toda informação produzida, recebida ou armazenada no âmbito do PRESERV constitui patrimônio público, essencial ao exercício de suas atribuições institucionais e, em última análise, à própria sustentabilidade do regime próprio de previdência social municipal.

É imperativo que toda informação sob custódia do PRESERV seja utilizada exclusivamente para os fins públicos e legítimos aos quais foi destinada, em estrita observância à legislação vigente, especialmente à Lei de Acesso à Informação (Lei nº 12.527/2011) e à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

Eventos como erros operacionais, fraudes, vandalismo, espionagem ou sabotagem podem resultar em modificação, divulgação indevida ou destruição não autorizada de informações, comprometendo a governança, a prestação de contas e a confiança da sociedade na administração pública. Por isso, constitui diretriz institucional proteger todos os ativos informacionais do PRESERV contra riscos e ameaças que possam afetar sua **confidencialidade** (respeitando restrições legais), **integridade** (assegurando exatidão e autenticidade) e **disponibilidade** (garantindo acesso oportuno a agentes autorizados no desempenho de suas funções públicas).

2.2 RESPONSABILIDADES

É missão institucional e responsabilidade indelegável do Instituto de Previdência Social dos Servidores Públicos Municipais – PRESERV garantir a adequada proteção das informações sob sua custódia. Essa responsabilidade estende-se a todos os agentes que, direta ou indiretamente, atuam em seu nome ou em suas dependências — incluindo servidores públicos, estagiários, prestadores de serviços, conselheiros, parceiros institucionais e visitantes. Todos devem conhecer, observar e cumprir as políticas, padrões, procedimentos e orientações estabelecidos nesta Política de Segurança da Informação.

Na administração pública, a segurança da informação não é apenas uma questão técnica, mas um compromisso ético e legal com a proteção do patrimônio público, a transparência e a prestação de contas à sociedade. Por isso, é imprescindível que cada indivíduo compreenda o papel que desempenha na salvaguarda das informações em suas atividades cotidianas, atuando sempre com zelo, responsabilidade e respeito aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência.

Todas as ações desenvolvidas no âmbito do PRESERV — por servidores, estagiários ou demais colaboradores — devem estar em plena conformidade

com a legislação vigente, em especial com a Lei de Acesso à Informação (Lei nº 12.527/2011), a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), bem como com as normas e diretrizes emitidas por órgãos de controle, fiscalização e regulação competentes. A aderência a esses marcos legais e normativos é condição essencial para a integridade, a confiabilidade e a continuidade dos serviços públicos prestados pelo Instituto.

2.3 INFORMAÇÕES CONFIDENCIAIS

Para os fins desta Política de Segurança da Informação, consideram-se **informações confidenciais** todos os dados, documentos e materiais — em qualquer formato, suporte ou meio (físico, digital, oral ou outro) — que, por força de lei, regulamento ou natureza funcional, não sejam de acesso público ou estejam sujeitos a restrições legais de uso e divulgação. Isso inclui, mas não se limita a: dados pessoais protegidos pela Lei Geral de Proteção de Dados (LGPD), informações sigilosas ou reservadas, especificações técnicas, projetos, estudos, relatórios internos, manuais operacionais, comunicações institucionais, arquivos eletrônicos, programas de computador, esboços, modelos e demais ativos informacionais sob custódia do Instituto de Previdência Social dos Servidores Públicos Municipais – PRESERV.

A responsabilidade pela observância rigorosa desta Política recai sobre todos os agentes que, a qualquer título, atuam em nome ou nas dependências do PRESERV: servidores públicos, estagiários, prestadores de serviços, conselheiros, parceiros institucionais e visitantes. Esses atores devem tratar as informações confidenciais com o máximo zelo, em estrita conformidade com os princípios da administração pública e a legislação vigente.

É vedada a divulgação, transferência ou compartilhamento de quaisquer informações confidenciais com terceiros sem prévia e expressa autorização por escrito do PRESERV. Qualquer revelação autorizada deverá ocorrer

exclusivamente nos termos e condições estabelecidos pelo Instituto, respeitando os limites legais e a finalidade pública a que se destina.

As informações confidenciais deverão ser utilizadas tão somente para o exercício das atribuições institucionais do PRESERV, dentro do território nacional e em estrita observância ao interesse público.

Caso ocorra qualquer uso indevido, acesso não autorizado, perda, vazamento ou outra violação que implique descumprimento desta Política, o servidor ou agente envolvido tem o dever funcional e ético de comunicar imediatamente o fato à autoridade competente do PRESERV, para adoção das providências cabíveis.

Não se aplicam à obrigação de confidencialidade as seguintes situações, desde que em conformidade com o ordenamento jurídico:

1. **Cumprimento de ordem judicial ou determinação legal** emanada de autoridade competente, incluindo atos do Poder Judiciário, Legislativo, tribunais arbitrais ou órgãos da administração pública com atribuições legais de fiscalização ou controle;

2. **Compartilhamento necessário com agentes públicos, representantes institucionais** (tais como advogados, auditores externos, peritos ou consultores técnicos) **devidamente autorizados**, quando imprescindível ao exercício das funções do PRESERV;

3. **Divulgação expressamente autorizada por escrito pelo PRESERV**, observadas as condições e limitações estabelecidas.

Em todos os casos, prevalece o primado da legalidade e o respeito aos direitos fundamentais, especialmente à privacidade, à proteção de dados pessoais e à transparência da administração pública.

3. PRINCÍPIOS E DIRETIVAS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

3.1 CLASSIFICAÇÃO DA INFORMAÇÃO

As informações e os sistemas de informação, diretórios de rede e bancos de dados são classificados como estritamente confidenciais.

As informações, seja no período de geração, guarda uso, transferência e destruição devem ser tratadas em conformidade com cada etapa do ciclo. As informações confidenciais necessitam de sigilo absoluto e devem ser protegidas de alterações não autorizadas e estarem disponíveis apenas às pessoas pertinentes e autorizadas a trabalhá-las, sempre que necessário.

Falhas no sigilo da informação, integridade ou disponibilidade deste tipo de informação trazem grandes prejuízos à Organização, expressos em perdas financeiras diretas, perdas de competitividade e produtividade ou imagem do PRESERV, podendo levar à extinção das operações ou prejuízos graves ao crescimento.

São exemplos de informações confidenciais:

✓ Informações de segurados ativos, inativos e de seus dependentes que devem ser protegidas por obrigatoriedade legal, incluindo dados cadastrais (CPF, RG etc.), situação financeira e movimentação bancária; - Informações sobre produtos e serviços que revelem vantagens competitivas do PRESERV frente ao mercado;

✓ Todo o material institucional do PRESERV (material impresso, armazenado em sistemas ou em mensagens eletrônicas) relacionados a sua atividade fim.

✓ Quaisquer informações do PRESERV, que não devem ser divulgadas ao meio externo antes da publicação pelas áreas competentes;

✓ Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades. Estas informações são também pessoais e intransferíveis.

3.2 ACESSO A SISTEMAS E RECURSOS DE REDE

O servidor do PRESERV é totalmente responsável pela correta posse e utilização de suas senhas e autorizações de acesso a sistemas, assim como pelas ações decorrentes da utilização destes poderes. O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções. Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados. A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função.

3.3 UTILIZAÇÃO DOS RECURSOS DE INFORMAÇÃO

A utilização dos recursos de informação do RPPS PRESERV deve observar rigorosos critérios de segurança e conformidade. Somente equipamentos e softwares previamente disponibilizados, autorizados ou homologados pelo PRESERV podem ser instalados ou conectados à sua rede corporativa, garantindo a integridade, confidencialidade e disponibilidade dos dados institucionais.

Todos os ativos de informação — sejam eles físicos ou digitais — devem ser tratados com o devido cuidado e proteção. Especial atenção deve ser dada a documentos impressos, mídias removíveis (como pen drives, HDs externos, CDs, entre outros) e quaisquer suportes que contenham dados sensíveis ou restritos. Esses materiais devem ser armazenados em locais seguros, de acesso

controlado, e jamais deixados desacompanhados ou expostos em ambientes não autorizados.

Além disso, é vedado o descarte inadequado de documentos após sua cópia, impressão ou uso. Todo material contendo informações institucionais deve ser devidamente armazenado, descartado de forma segura (por meio de destruição física ou digital, conforme o caso) ou devolvido ao seu local de origem, conforme as políticas internas de gestão da informação e segurança da informação do PRESERV.

3.4 AUTENTICAÇÃO E SENHA

O servidor do PRESERV é integralmente responsável por todos os atos realizados por meio de seu identificador único (login/sigla) e respectiva senha, os quais constituem mecanismos exclusivos de autenticação individual para acesso às informações institucionais e aos recursos de tecnologia da informação.

Diante disso, todos os colaboradores do PRESERV devem observar rigorosamente as seguintes orientações de segurança:

- Manter a confidencialidade da senha: memorizá-la e jamais registrá-la em qualquer suporte físico ou digital — como papéis, arquivos de texto, planilhas ou dispositivos móveis — nem compartilhá-la com terceiros, mesmo que sejam colegas de trabalho ou superiores hierárquicos.

- Alterar imediatamente a senha sempre que houver qualquer indício ou suspeita de comprometimento, como acesso não autorizado, uso indevido ou perda de controle sobre a credencial.

- Utilizar senhas robustas, compostas por combinações complexas de letras (maiúsculas e minúsculas), números e caracteres especiais, evitando informações pessoais, sequências previsíveis ou padrões facilmente adivinháveis.

- Não permitir o uso de seu equipamento por terceiros enquanto estiver autenticado em sistemas ou redes institucionais, garantindo que apenas ele tenha acesso sob sua identidade.

- Bloquear a sessão do equipamento sempre que se ausentar, utilizando o comando de bloqueio (por exemplo, Ctrl + Alt + Del e selecionando “Bloquear” no ambiente Windows), evitando acessos indevidos durante sua ausência temporária.

O descumprimento dessas diretrizes poderá implicar responsabilização administrativa, conforme as normas internas do PRESERV e a legislação vigente, considerando o alto grau de sensibilidade das informações sob sua guarda.

4. PASTAS COMPARTILHADAS E CÓPIA DE SEGURANÇA

Cada setor do PRESERV deve realizar, de forma contínua e sistemática, o levantamento e a organização dos documentos relevantes às suas finalidades institucionais, observando os princípios da finalidade, necessidade e adequação previstos na Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018). Tais documentos deverão ser armazenados de maneira estruturada, podendo ser classificados em pastas departamentais, por processos administrativos ou em repositórios públicos internos, e compartilhados na rede institucional apenas quando justificado pela execução de atividades legítimas do PRESERV.

Todos os setores deverão disponibilizar todos os arquivos institucionais armazenados em pastas compartilhadas diretamente no servidor, a fim de

realizar backups periódicos, assegurando a integridade, confidencialidade e disponibilidade das informações — medidas essenciais para o cumprimento do dever legal de segurança no tratamento de dados previsto no Art. 46 da LGPD.

Cabe a cada usuário a responsabilidade de manter cópias de segurança locais (em sua estação de trabalho) dos arquivos sob sua guarda, como medida complementar de proteção contra perda acidental, especialmente quando se tratar de dados pessoais ou sensíveis.

Destaca-se que arquivos não vinculados aos processos do PRESERV — tais como documentos de cunho pessoal, arquivos temporários ou conteúdos alheios às finalidades institucionais — não devem ser armazenados em servidores centralizados nem incluídos nas rotinas oficiais de backup. O compartilhamento eventual entre colaboradores desses materiais não descaracteriza a vedação ao seu armazenamento institucional, conforme o princípio da necessidade (Art. 6º, II, da LGPD), que exige a limitação do tratamento ao mínimo indispensável para as finalidades pretendidas.

O descumprimento destas diretrizes poderá comprometer a segurança da informação, expor o PRESERV a riscos legais e administrativos e implicar responsabilização individual ou coletiva, nos termos da legislação vigente, incluindo as sanções previstas pela Autoridade Nacional de Proteção de Dados (ANPD).

5. LEIS E REGULAMENTOS

É responsabilidade de todos os colaboradores do PRESERV conhecer, compreender e cumprir integralmente a legislação aplicável, incluindo as normas, regulamentos e padrões locais, estaduais e federais em vigor — em especial a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) —, bem como as políticas, diretrizes e procedimentos internos institucionais.

6. RESPONSABILIDADES E DISPOSIÇÕES FINAIS

Esta política mantém sua aplicabilidade mesmo após o desligamento do servidor ou o encerramento do contrato com terceiros, permanecendo vigentes as obrigações de confidencialidade, sigilo e proteção das informações a que tenham tido acesso durante a vigência do vínculo. Tais responsabilidades persistem enquanto os envolvidos puderem ser responsabilizados — administrativa, civil ou criminalmente — por atos praticados no exercício de suas funções.

Ao tomar ciência desta política, servidores e terceiros expressamente assumem o compromisso de não divulgar, reproduzir, transferir ou utilizar, por qualquer meio — lícito ou ilícito —, dados sensíveis, pessoais ou restritos sob custódia do RPPS PRESERV, inclusive após o término de seu vínculo institucional. Igualmente, obrigam-se a garantir a guarda segura e o tratamento adequado de todas as informações confiadas, em conformidade com os princípios da segurança, finalidade e necessidade estabelecidos na Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) e demais normas aplicáveis.

7. CONTROLE DE VERSÕES

Elaborado por	Revisado por	Aprovado por	Versão	Aprovado em
Controladora da Previdência, Miriane Batista	Comissão do Pró-Gestão	Comissão do Pró-Gestão	1.0	12/12/2025

TERMO DE COMPROMISSO PARA SERVIDORES E CONSELHEIROS DO PRESERV

Declaro que li, compreendi e estou plenamente de acordo com a Política de Segurança da Informação do PRESERV, disponível na página eletrônica oficial: https://www.preserv.mg.gov.br, tendo pleno conhecimento de seu teor integral e das obrigações por ela estabelecidas.

Declaro, ainda, que estou ciente de que a prática de quaisquer atos em desacordo com a referida política — especialmente no que diz respeito ao uso inadequado de sistemas, acesso não autorizado, vazamento ou descuido com informações institucionais — poderá resultar na adoção de medidas disciplinares, administrativas, civis ou criminais, podendo culminar, conforme a gravidade da infração, no desligamento do quadro efetivo de servidores da PRESERV, na perda do mandato no Conselho, na responsabilização perante a Autoridade Nacional de Proteção de Dados (ANPD) ou na propositura de ações judiciais.

Comprometo-me, de forma irrevogável, a preservar, durante e após o término do meu vínculo com o PRESERV, a confidencialidade, integridade e disponibilidade de todas as informações, dados e documentos a que tiver acesso em razão de minhas atribuições, observando os princípios da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e demais normas aplicáveis.

PREENCHIMENTO PELO SERVIDOR/CONSELHEIRO:

Nome: _____

CPF:_____

Cargo:_____

E-mail:_____

Data: _____/_____/_____

Assinatura: _____

TERMO DE COMPROMISSO PARA TERCEIROS/PRESTADORES DE SERVIÇO AO PRESERV

Declaro que li, compreendi e estou plenamente de acordo com a Política de Segurança da Informação do PRESERV, disponível na página eletrônica oficial: https://www.preserv.mg.gov.br, tendo pleno conhecimento de seu teor integral e das obrigações nela estabelecidas, especialmente no que se refere ao tratamento adequado de dados, uso de sistemas e proteção de ativos de informação.

Declaro, ainda, estar ciente de que a prática de quaisquer atos em desacordo com a referida política — tais como uso indevido de sistemas, acesso não autorizado, vazamento, perda, compartilhamento não autorizado ou descuido com informações institucionais ou pessoais — poderá ensejar a rescisão imediata do contrato ou vínculo de prestação de serviços, além da adoção de medidas administrativas, civis ou criminais, conforme a gravidade da infração. Tais medidas incluem, mas não se limitam à, responsabilização perante a Autoridade Nacional de Proteção de Dados (ANPD) e à propositura de ações judiciais por danos materiais ou morais.

Comprometo-me, de forma irrevogável e vinculante, a preservar, durante e após o término da minha prestação de serviços ao PRESERV, a confidencialidade, integridade e disponibilidade de todas as informações, dados e documentos aos quais tiver acesso em razão de minhas atividades, observando rigorosamente os princípios da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), demais normas aplicáveis e as cláusulas contratuais firmadas com o PRESERV.

PREENCHIMENTO PELO TERCEIRO/PRESTADOR DE SERVIÇO:

Empresa: _____

Responsável: _____

CPF: _____

Cargo:_____

Telefone: ( ) _____

E-mail: _____

Data: _____/_____/_____

Assinatura: _____

APROVAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO PRESERV - VERSÃO 1.0

COMISSÃO DO PRÓ-GESTÃO

Brenda Karollyne Silva
Analista Previdenciária – Função Jurídico

Eleni Soares Santos André
Diretora de Benefícios e Atuária

Heberton da Silva Tolentino
Assessor Jurídico

Hermak Pires de Oliveira
Diretor de Administração e Finanças

Miriane Aparecida Batista
Controladora da Previdência

SUPERINTENDENTE EXECUTIVO DO PRESERV

Geraldo Batista Filho
Superintendente Executivo