PARANAGUÁ
PREVIDÊNCIA

Política de Segurança da Informação PARANAGUAPREV

SUMÁRIO

1. OBJETIVO

A presente Política de Segurança da Informação (PSI) tem por objetivo estabelecer diretrizes, princípios, responsabilidades e controles mínimos necessários para a proteção das informações sob a guarda da Paranaguá Previdência, assegurando a confidencialidade, a integridade, a disponibilidade, a legalidade e a rastreabilidade das informações, em conformidade com a legislação vigente e com as boas práticas aplicáveis à Administração Pública.

Esta Política visa orientar o uso adequado dos ativos de informação, sejam eles físicos ou digitais, próprios ou terceirizados, prevenindo acessos não autorizados, vazamentos de dados, indisponibilidades de sistemas, perdas de informação e outros incidentes que possam comprometer a continuidade das atividades institucionais, a proteção dos dados pessoais dos segurados, servidores e demais titulares, bem como a imagem e a credibilidade da Paranaguá Previdência.

Considerando a realidade organizacional e tecnológica da entidade, caracterizada pela inexistência de estrutura própria de Tecnologia da Informação e pela utilização predominante de sistemas, serviços e infraestrutura terceirizados, esta Política estabelece controles proporcionais, viáveis e compatíveis com o porte da instituição, atribuindo responsabilidades claras aos usuários internos e aos prestadores de serviços contratados, sem impor exigências técnicas incompatíveis com sua capacidade operacional.

A PSI constitui instrumento fundamental de governança, integrando-se aos processos administrativos, aos contratos firmados com terceiros, às ações de proteção de dados pessoais e às exigências do Programa Pró-Gestão RPPS, servindo como referência obrigatória para a tomada de decisões relacionadas à segurança da informação e à gestão de riscos informacionais no âmbito da Paranaguá Previdência.

2. ABRANGÊNCIA

Aplica-se a:

- Servidores públicos;
- Estagiários;
- Prestadores de serviço;
- Empresas contratadas para fornecimento de sistemas, suporte técnico, hospedagem, e-mail e armazenamento em nuvem;
- Qualquer pessoa que tenha acesso, ainda que eventual, às informações da Paranaguá Previdência.

3. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

A PSI fundamenta-se nos seguintes princípios:

- Confidencialidade
- Integridade
- Disponibilidade
- Legalidade e Finalidade
- Responsabilização e Prestação de Contas

4. GOVERNANÇA E RESPONSABILIDADES

4.1 Alta Administração

Compete à Presidência:

- Aprovar esta Política;

- Garantir sua divulgação;
- Assegurar cláusulas contratuais de segurança da informação;
- Designar responsável formal pela gestão da PSI.

4.2 Responsável pela Segurança da Informação

A gestão da PSI será exercida por responsável formalmente designado, podendo acumular funções administrativas, não sendo exigida estrutura própria de TI.

Compete:

- Coordenar a aplicação da PSI;
- Interagir com prestadores de serviço;
- Acompanhar incidentes e revisões.

4.3 Infraestrutura de TI

A Paranaguá Previdência não possui estrutura própria de TI, sendo:

- A infraestrutura local (servidor de domínio e arquivos) administrada por empresa terceirizada
- O suporte técnico aos usuários integralmente terceirizado
- Os sistemas previdenciários e administrativos totalmente externos

As responsabilidades técnicas recaem sobre os prestadores contratados, conforme cláusulas específicas.

4.4 Usuários

Compete aos usuários:

- Utilizar sistemas apenas para fins institucionais;
- Manter sigilo das credenciais;
- Comunicar incidentes;
- Cumprir esta Política.

5. CONTROLE DE ACESSO

O controle de acesso tem como objetivo assegurar que apenas pessoas autorizadas tenham acesso às informações, sistemas e ambientes da Paranaguá Previdência, preservando a confidencialidade, integridade e disponibilidade dos dados institucionais.

Considerando a estrutura organizacional reduzida da entidade e a inexistência de setor próprio de Tecnologia da Informação, o controle de acesso é realizado de forma administrativa, com apoio dos prestadores de serviços responsáveis pelos sistemas utilizados pela instituição.

5.1 Princípios Gerais

O controle de acesso observará os seguintes princípios:

- Utilização de credenciais individuais e intransferíveis;
- Concessão de acesso conforme necessidade funcional (princípio do menor privilégio);
- Registro e rastreabilidade das solicitações de acesso;
- Bloqueio imediato em caso de desligamento ou alteração de função;
- Responsabilidade do usuário pela guarda e sigilo de suas credenciais.

É vedado o compartilhamento de logins ou senhas entre usuários.

5.2 Responsável pela Gestão de Acessos

A gestão administrativa e operacional dos acessos aos sistemas institucionais é exercida pela Diretoria Administrativa, atualmente representada pela servidora Luciana Camargo Franco, que possui perfis

administrativos ou de gestão de usuários, quando disponibilizados pelos sistemas utilizados pela instituição.

Compete à responsável:

- Avaliar a necessidade funcional do acesso solicitado;
- Autorizar ou negar solicitações de criação, alteração ou exclusão de acessos;
- Realizar, sempre que possível, a criação, alteração ou bloqueio de usuários diretamente nos sistemas institucionais;
- Solicitar suporte técnico às empresas fornecedoras dos sistemas quando necessário, especialmente em situações que demandem orientação técnica ou intervenção especializada;
- Acompanhar situações de desligamento, afastamento ou mudança de função que exijam revisão dos acessos concedidos.

Os prestadores de serviços de tecnologia atuam exclusivamente em caráter de suporte técnico, não sendo responsáveis pela decisão administrativa de concessão de acessos.

5.3 Procedimento de Concessão de Acesso Lógico

A concessão de acesso aos sistemas institucionais seguirá, sempre que aplicável, as seguintes etapas:

1. O servidor ou setor demandante solicita o acesso necessário para execução de suas atividades institucionais;
2. A solicitação é analisada pela Diretoria Administrativa, que verifica a necessidade funcional do acesso;
3. Uma vez autorizada a solicitação, a responsável realiza a criação ou configuração do acesso diretamente no sistema correspondente, utilizando suas credenciais administrativas;
4. Caso haja necessidade de apoio técnico, poderá ser solicitado suporte ao fornecedor do sistema ou à empresa responsável pelo suporte tecnológico;
5. O usuário recebe suas credenciais de acesso e deverá realizar a troca de senha no primeiro acesso, sempre que o sistema permitir.

Os perfis de acesso deverão refletir exclusivamente as atividades desempenhadas pelo usuário, observando o princípio do menor privilégio.

5.4 Alteração ou Revogação de Acessos

Sempre que ocorrer:

- Mudança de função;
- Afastamento prolongado;
- Desligamento do servidor;
- Encerramento de contrato de prestador de serviço,

a Diretoria Administrativa deverá proceder à alteração, suspensão ou exclusão dos acessos existentes.

Essas medidas serão realizadas diretamente nos sistemas institucionais pela responsável pela gestão de acessos, podendo haver apoio técnico das empresas fornecedoras dos sistemas quando necessário.

5.5 Controle de Acesso Físico

O acesso às dependências administrativas da Paranaguá Previdência é restrito aos servidores, colaboradores autorizados e prestadores de serviço.

Visitantes deverão:

- Identificar-se na recepção ou setor responsável;

- Informar o motivo da visita;
- Permanecer acompanhados por servidor durante a permanência nas dependências da instituição.

Ambientes que contenham equipamentos, documentos ou arquivos institucionais devem permanecer sob responsabilidade dos servidores autorizados.

5.6 Responsabilidades dos Usuários

Todos os usuários que possuam acesso aos sistemas ou informações institucionais devem:

- Manter sigilo sobre suas credenciais;
- Não compartilhar logins ou senhas;
- Bloquear o computador quando se ausentar da estação de trabalho;
- Comunicar imediatamente qualquer suspeita de uso indevido de acesso ou incidente de segurança.

6. USO DE INTERNET, E-MAIL E SISTEMAS

- Uso exclusivamente institucional;
- Vedado compartilhamento de senhas;
- Vedado armazenamento de dados institucionais em nuvens pessoais;
- O e-mail institucional e o site são serviços terceirizados, devendo observar boas práticas de segurança.

7. BACKUP E CONTINUIDADE

- O servidor local possui backup em nuvem;
- Os sistemas terceirizados devem manter backup próprio;
- A Paranaguá Previdência mantém mapeamento dos responsáveis por backup, sem operação direta.

Não há obrigação de plano próprio de DRP interno, em razão da estrutura reduzida.

8. INCIDENTES DE SEGURANÇA

Considera-se incidente qualquer evento que comprometa dados ou sistemas.

Todo incidente deverá:

- Ser comunicado imediatamente;
- Ser registrado;
- Ter providências adotadas em conjunto com o prestador responsável.

Incidentes envolvendo dados pessoais seguirão a LGPD.

9. TERCEIROS E CONTRATOS

Todos os contratos deverão conter:

- Cláusulas de confidencialidade;
- Obrigações de segurança;
- Comunicação imediata de incidentes;
- Responsabilidade como operadores de dados, quando aplicável.

10. LGPD E PROTEÇÃO DE DADOS

- A Paranaguá Previdência atua como controladora de dados

- Os sistemas terceirizados atuam como operadores
- Existe Encarregado de Dados designado
- Os direitos dos titulares são assegurados

11. TREINAMENTO E CONSCIENTIZAÇÃO

- Orientações básicas na admissão;
- Divulgação anual da PSI;
- Não há exigência de programas complexos ou ferramentas especializadas.

12. VIGÊNCIA, REVISÃO E CONTROLE DE VERSÃO

- Revisão a cada 2 anos ou quando necessário;
- Histórico de versões mantido ao final do documento;
- Cópias impressas são não controladas.

13. DISPOSIÇÕES FINAIS

Por fim, reforçamos que esta Política de Segurança da Informação existe para proteger a Paranaguá Previdência e todos os seus stakeholders (servidores, beneficiários, fornecedores e sociedade em geral) contra riscos relacionados à informação. Cada um de nós tem um papel na manutenção de um ambiente seguro. Com a cooperação de todos no cumprimento fiel destas diretrizes, somada ao apoio contínuo da administração, conseguiremos preservar a confiabilidade, a imagem e a excelência dos serviços prestados por esta instituição, em conformidade com as melhores práticas internacionais e com a legislação brasileira vigente.

Paranaguá, 15 de janeiro de 2026.

HISTÓRICO DE VERSÕES

Versão	01
Data de vigência	15/01/2026
Elaborado por	Luciana Camargo Franco
Aprovado por	Presidente – Ali El Kadri
Próxima revisão prevista	15/01/2028