

Instituto de Previdência dos Servidores Públicos do Município de Piracaia - PIRAPREV

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

Versão	Data	Descrição da Alteração	Elaborador	Aprovado Por
1.0	16/08/2023	Aprovação inicial da Política de Segurança da Informação (PSI).	Superintendência	Conselho Administrativo
2.0	15/09/2026	1. Adequação aos requisitos do Pró-Gestão RPPS – Nível III. 2. Redistribuição de competências para a Superintendência, Gestão de SI e TI. 3. Revisão a cada 4 anos	Superintendência	Conselho Administrativo

CAPÍTULO I – OBJETIVOS E PRINCÍPIOS DA PSI

Art. 1º. A Política de Segurança da Informação, também referida como PSI, estabelece as diretrizes do PIRAPREV para a proteção dos ativos de informação e define responsabilidades aplicáveis a todos os usuários, servidores, colaboradores, membros dos órgãos colegiados e prestadores de serviços que tenham acesso às informações de propriedade ou sob guarda do RPPS.

Art. 2º. Constituem objetivos da PSI:

I – estabelecer diretrizes que permitam aos usuários e prestadores de serviços seguir padrões de comportamento relacionados à segurança da informação adequados às necessidades do PIRAPREV e à proteção legal da instituição e dos titulares das informações;
II – nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento, observada a legislação aplicável, inclusive a Lei nº 13.709/2018 – LGPD;
III – preservar as informações do PIRAPREV quanto à confidencialidade, integridade e disponibilidade;
IV – estabelecer responsabilidades e procedimentos para prevenção, identificação, tratamento e recuperação de incidentes de segurança da informação;
V – promover a continuidade e a recuperação dos serviços e informações essenciais ao funcionamento do RPPS.

Art. 3º. A segurança da informação observará, no mínimo, os seguintes princípios:

I – Confidencialidade: proteção e garantia de que determinadas informações somente estejam disponíveis às pessoas autorizadas;
II – Integridade: garantia da exatidão, completude e preservação das informações e dos métodos de processamento contra alterações indevidas, intencionais ou acidentais;
III – Disponibilidade: garantia de que usuários autorizados tenham acesso às informações e aos recursos necessários sempre que deles necessitarem.

CAPÍTULO II – APLICAÇÃO E RESPONSABILIDADES GERAIS

Art. 4º. As diretrizes desta PSI aplicam-se a todas as áreas do PIRAPREV, às informações em qualquer meio ou suporte e a todos os servidores, colaboradores, dirigentes, membros dos Conselhos, membros do Comitê de Investimentos e prestadores de serviços que tenham acesso a informações ou recursos tecnológicos do RPPS.

Art. 5º. É obrigação de cada usuário manter-se atualizado em relação a esta PSI e aos procedimentos e normas dela decorrentes, buscando orientação sempre que houver dúvida quanto à aquisição, acesso, utilização, compartilhamento, armazenamento ou descarte de informações.

Art. 6º. Os usuários deverão:

I – manter sigilo das informações a que tiverem acesso em razão de suas atividades;
II – zelar pelos ativos físicos e digitais de informação do PIRAPREV;
III – utilizar os recursos tecnológicos exclusivamente de acordo com as normas institucionais;
IV – comunicar imediatamente à área responsável qualquer incidente, suspeita de incidente, perda, acesso indevido ou vulnerabilidade de segurança de que tenham conhecimento;
V – observar as regras de proteção de dados pessoais e demais normas legais aplicáveis.

CAPÍTULO III – RESPONSABILIDADES ESPECÍFICAS

Art. 7º. Compete à Superintendência:

I – aprovar e promover a aplicação desta PSI;
II – assegurar condições administrativas para sua implementação;
III – designar, quando necessário, responsáveis pela execução dos procedimentos de segurança da informação;
IV – deliberar sobre medidas corretivas, de aprimoramento e estratégias necessárias à implantação, manutenção e revisão desta PSI e das normas complementares.

Art. 8º. Compete ao responsável pela Gestão de Segurança da Informação:

I – prover, consolidar e manter atualizadas as informações relacionadas à Gestão de Segurança da Informação do PIRAPREV;
II – coordenar a aplicação dos procedimentos previstos nesta PSI;
III – acompanhar incidentes, riscos, controles e ações corretivas;
IV – elaborar e atualizar as normas e procedimentos de segurança, bem como propor a revisão desta PSI sempre que necessário;
V – prestar informações e relatórios à Superintendência;
VI – propor e acompanhar ações de conscientização, capacitação, projetos e melhorias relacionadas à segurança da informação;
VII – acompanhar a classificação das informações e os prazos de guarda em conjunto com os setores responsáveis.

Art. 9º. Compete aos usuários cumprir as diretrizes desta PSI e comunicar ocorrências de segurança.

Art. 10. A área de Tecnologia da Informação do PIRAPREV ou o prestador de serviços contratado será responsável, conforme suas atribuições contratuais ou internas, pela execução dos procedimentos técnicos de segurança, contingência, cópias de segurança, recuperação, controle de acesso, bem como por auxiliar no acompanhamento dos resultados das auditorias de acesso lógico e testes de recuperação de desastres.

Art. 11. A PSI deverá ser revisada periodicamente, no mínimo a cada 4 (quatro) anos, ou sempre que houver alteração relevante nos processos, sistemas, riscos, legislação ou estrutura do PIRAPREV.

CAPÍTULO IV – MONITORAMENTO, AUDITORIA E INCIDENTES

Art. 12. O PIRAPREV poderá utilizar mecanismos de monitoramento das estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis, sistemas e demais componentes tecnológicos, observada a legislação aplicável.

Art. 13. Os registros de acesso e de eventos de segurança poderão ser utilizados para identificação de ocorrências, auditoria, investigação de incidentes e aperfeiçoamento dos controles, respeitados os direitos dos titulares e as normas de proteção de dados.

Art. 14. Os incidentes ou suspeitas de incidentes deverão ser comunicados à área responsável, registrados e avaliados quanto à necessidade de contenção, correção, recuperação e comunicação às instâncias competentes.

Art. 15. O procedimento de auditoria de acesso lógico deverá, no mínimo, contemplar:

I – verificação periódica dos usuários ativos e respectivos perfis de acesso;
II – verificação de acessos incompatíveis com as funções exercidas;

III – conferência de acessos de usuários desligados, afastados ou que tenham mudado de função;
IV – análise, quando disponível, de registros de acesso, tentativas indevidas e eventos relevantes;
V – registro das ocorrências identificadas e das providências adotadas;
VI – manutenção das evidências da auditoria pelo prazo definido na classificação e temporalidade documental.

CAPÍTULO V – CORREIO ELETRÔNICO

Art. 16. O uso do correio eletrônico do PIRAPREV destina-se às atividades institucionais. É vedado, entre outros:

I – enviar mensagens não solicitadas para múltiplos destinatários, salvo quando relacionadas a atividade legítima do RPPS;
II – utilizar a identidade ou endereço de outro usuário sem autorização;
III – enviar conteúdo que exponha o PIRAPREV ou terceiros a riscos jurídicos ou de segurança;
IV – divulgar informações, documentos ou imagens sem autorização;
V – falsificar informações de endereçamento ou cabeçalhos;
VI – eliminar mensagens pertinentes quando o RPPS estiver sujeito a investigação ou obrigação de preservação.

CAPÍTULO VI – INTERNET, COMPUTADORES E DISPOSITIVOS

Art. 17. Os recursos tecnológicos e o acesso à internet, disponibilizados pelo PIRAPREV destinam-se prioritariamente às atividades institucionais e deverão ser utilizados de forma ética, profissional e segura.

Art. 18. O PIRAPREV poderá bloquear arquivos, sites, domínios, aplicações ou conteúdos que representem risco à segurança ou contrariem esta PSI, observada a legislação aplicável.

Art. 19. É vedado utilizar os recursos do RPPS para atividades ilícitas, disseminação de códigos maliciosos, assédio, acesso ou armazenamento de conteúdo incompatível com as finalidades institucionais ou instalação de software sem autorização.

Art. 20. Os computadores e demais dispositivos disponibilizados pelo PIRAPREV constituem instrumentos de trabalho e deverão ser protegidos contra uso indevido, perda, furto, acesso não autorizado e instalação de recursos não autorizados.

CAPÍTULO VII – CONTROLE DE ACESSO LÓGICO

Art. 21. O acesso aos recursos tecnológicos do PIRAPREV deverá utilizar, sempre que tecnicamente possível, identificação individual e senha exclusiva de cada usuário.

§ 1º. É proibido o compartilhamento de credenciais.
§ 2º. O usuário deverá proteger suas credenciais e comunicar imediatamente suspeita de comprometimento.
§ 3º. Os perfis de acesso deverão observar o princípio do menor privilégio, de acordo com as necessidades das funções exercidas.
§ 4º. A concessão, alteração, suspensão e revogação de acessos deverão ser registradas de acordo com procedimento próprio.
§ 5º. Usuários desligados ou que deixarem de necessitar de determinado acesso deverão ter suas credenciais revogadas ou ajustadas tempestivamente.

CAPÍTULO VIII – CONTROLE DE ACESSO FÍSICO

Art. 22. O acesso físico às dependências do PIRAPREV e às áreas que contenham equipamentos, documentos ou informações sensíveis deverá ser controlado de acordo com o nível de risco e a natureza da informação.

Art. 23. O acesso a áreas restritas, especialmente locais destinados a equipamentos de tecnologia, documentos ou infraestrutura crítica, deverá ser limitado às pessoas autorizadas.

Art. 24. Visitantes e prestadores de serviços deverão observar as regras de acesso e, quando aplicável, permanecer acompanhados ou autorizados por servidor responsável.

Art. 25. Chaves, cartões, dispositivos de acesso e demais mecanismos de controle físico deverão ser mantidos sob responsabilidade de pessoa ou área definida pelo PIRAPREV, com registro e revogação quando necessário.

CAPÍTULO IX – CLASSIFICAÇÃO DA INFORMAÇÃO E TEMPORALIDADE

Art. 26. As informações sob guarda do PIRAPREV deverão ser classificadas considerando seu grau de sensibilidade, necessidade de acesso, impacto decorrente de divulgação indevida e legislação aplicável.

Art. 27. Para fins de segurança da informação, poderão ser adotadas as seguintes classificações:

I – Pública: informação cuja divulgação seja permitida e não gere prejuízo à instituição ou a terceiros;
II – Interna: informação destinada ao uso no âmbito institucional, cuja divulgação externa não seja necessária;
III – Restrita: informação cujo acesso deve ser limitado a pessoas ou áreas determinadas em razão de suas atribuições;
IV – Confidencial: informação cujo acesso indevido possa causar dano relevante ao PIRAPREV, aos segurados, beneficiários, servidores ou terceiros.

Art. 28. A classificação deverá ser acompanhada da definição do prazo de guarda e da destinação da informação, observada a legislação, as obrigações de transparência, a LGPD e os instrumentos de gestão documental aplicáveis.

§ 1º. O PIRAPREV manterá tabela ou instrumento complementar de classificação e temporalidade, com indicação das classes documentais, nível de acesso, prazo de guarda e destinação final.
§ 2º. Na inexistência de Arquivo Público ou estrutura equivalente no ente federativo para execução dos instrumentos de gestão documental, o PIRAPREV poderá contar com servidor do ente ou do RPPS designado para apoiar as ações de classificação da informação e definição do tempo de sua guarda.

CAPÍTULO X – DIVULGAÇÃO E CONSCIENTIZAÇÃO

Art. 29. O PIRAPREV promoverá ampla divulgação desta PSI e das normas complementares aos servidores, colaboradores e prestadores de serviços, inclusive por meios eletrônicos e/ou físicos.

Art. 30. O PIRAPREV promoverá, periodicamente, ações de conscientização e orientação sobre segurança da informação, contemplando, conforme os riscos identificados, temas como senhas, phishing, uso seguro do correio eletrônico, proteção de documentos, dispositivos, dados pessoais, incidentes e descarte seguro.

Parágrafo único. Deverão ser mantidos registros das ações realizadas, tais como materiais utilizados, comunicações, listas de presença, registros de participação ou outros documentos comprobatórios.

Art. 31. O PIRAPREV poderá desenvolver projetos, campanhas, treinamentos e incentivos destinados ao aperfeiçoamento contínuo da segurança da informação.

CAPÍTULO XI – PROCEDIMENTOS DE CONTINGÊNCIA E CÓPIAS DE SEGURANÇA

Art. 32. Para garantir a segurança da informação e a continuidade dos serviços, deverão ser realizadas cópias de segurança dos sistemas e respectivos bancos de dados utilizados pelo PIRAPREV.

§ 1º. As rotinas de cópia de segurança deverão, sempre que possível, ser automatizadas, realizadas em horários definidos e submetidas a verificações periódicas de execução e integridade.
§ 2º. As cópias de segurança deverão ser armazenadas de forma a reduzir o risco de acesso não autorizado, perda, corrupção ou destruição.
§ 3º. Os processos de realização, armazenamento, verificação e restauração das cópias de segurança deverão estar mapeados e manualizados.
§ 4º. A área responsável pelos procedimentos de contingência será a de Tecnologia da Informação do PIRAPREV ou o prestador de serviço contratado, conforme definido em instrumento próprio.

CAPÍTULO XII – RECUPERAÇÃO DE DESASTRES E CONTINUIDADE

Art. 33. O PIRAPREV deverá manter procedimento de recuperação de desastres destinado a restabelecer, de forma ordenada e segura, os sistemas, dados e serviços essenciais afetados por incidentes ou eventos que comprometam sua disponibilidade.

Art. 34. O procedimento de recuperação de desastres deverá contemplar, no mínimo:

I – identificação dos eventos que possam provocar indisponibilidade relevante;
II – definição das responsabilidades e forma de acionamento;
III – priorização dos sistemas e serviços essenciais;
IV – utilização e restauração das cópias de segurança;
V – validação da integridade dos dados e dos sistemas restaurados;
VI – comunicação interna e, quando cabível, externa sobre a indisponibilidade e a recuperação;
VII – registro do evento, das providências adotadas e das lições aprendidas;
VIII – realização periódica de testes ou verificações de recuperação, sempre que tecnicamente viável.

CAPÍTULO XIII – PROTEÇÃO DE DADOS E DESCARTE

Art. 35. A Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD deverá ser observada em todas as atividades de tratamento de dados pessoais realizadas pelo PIRAPREV.

Art. 36. O descarte de informações e mídias deverá observar a classificação da informação, os prazos de guarda e os procedimentos de segurança, de modo a impedir recuperação ou acesso indevido quando não houver obrigação de conservação.

CAPÍTULO XIV – NÃO CONFORMIDADES, MONITORAMENTO E MELHORIA CONTÍNUA

Art. 37. As não conformidades, vulnerabilidades, incidentes e recomendações identificadas em verificações, auditorias ou avaliações deverão ser registradas e acompanhadas até sua conclusão, sempre que aplicável.

Art. 38. O responsável pela Gestão de Segurança da Informação, em conjunto com a Superintendência, deverá acompanhar as providências adotadas e determinar medidas de melhoria quando identificadas deficiências relevantes.

Art. 39. As evidências de execução dos procedimentos de segurança da informação deverão ser mantidas de forma organizada, permitindo sua verificação em auditorias internas, externas e no processo de certificação do Pró-Gestão RPPS.

CAPÍTULO XV – DISPOSIÇÕES FINAIS

Art. 40. O descumprimento desta PSI poderá sujeitar o responsável às medidas administrativas previstas na legislação aplicável, sem prejuízo de outras responsabilidades.

Art. 41. As normas e procedimentos complementares decorrentes desta PSI deverão ser mantidos atualizados e compatíveis com os processos do PIRAPREV.

Art. 42. Esta Política deverá ser publicada na Internet, em local de fácil acesso, e permanecer disponível para consulta dos servidores, prestadores de serviços, segurados e demais interessados.

Art. 43. Esta Política entra em vigor na data de sua aprovação, revogando-se as disposições em contrário.

Piracaia, 15 de setembro de 2026.

Claudia Leoncio Martins
Superintendente

ANEXO I – INSTRUMENTOS E PROCEDIMENTOS COMPLEMENTARES

Para fins de implementação e comprovação dos requisitos de Segurança da Informação, o PIRAPREV deverá manter, conforme aplicável, os seguintes instrumentos complementares:

1. Procedimento de auditoria de acesso lógico;
2. Procedimento de controle de acesso físico;
3. Procedimento de cópias de segurança e restauração;
4. Procedimento/Plano de recuperação de desastres;
5. Tabela de classificação da informação e temporalidade;
6. Plano ou registro de ações de conscientização e capacitação;
7. Registro de incidentes e das providências adotadas;
8. Registros de revisão e atualização da PSI;
9. Evidências de publicação e divulgação da PSI.