Política de Segurança da Informação (PSI)

GUARATUBA PREVIDÊNCIA – GUARAPREV

Política de Segurança da Informação – PSI	**VERSÃO** **2026.1**	**SITUAÇÃO** **APROVADA EM 27/10/2026**

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

CONTROLE DA VERSÃO E TRAMITAÇÃO

Política de Segurança da Informação – PSI, revisão consolidada 2026.1. Minuta elaborada em outubro de 2026 para apreciação do Conselho do GUARAPREV. A aprovação, o ato de instituição e a vigência deverão ser registrados após a deliberação competente.

Identificação	Registro
Documento	Política de Segurança da Informação – PSI
Unidade gestora	Guaratuba Previdência – GUARAPREV
Versão / situação	2026.1 / Minuta para apreciação e aprovação
Referência institucional anterior	Portaria GUARAPREV nº 006, de 06 de outubro de 2023.
Documento operacional relacionado	Manual de Padronização dos Processos de Segurança da Informação, revisão 1.1, sujeito à compatibilização com esta PSI.
Deliberação do Conselho	Ata/resolução nº _____ | Data: ____/____/_____
Ato de instituição e publicação	Ato nº _____ | Publicação: _____
Início da vigência	Conforme ato de instituição, após a publicação exigida.

Natureza da revisão

A minuta mantém a organização temática da PSI anterior e consolida os ajustes discutidos com o GUARAPREV e com a TI. Os comandos normativos representam regras propostas para aprovação; não são declaração de que todos os controles já estejam implantados.

O prazo de 30 dias para apresentação do plano de adequação, o acompanhamento trimestral até sua conclusão e a avaliação anual da PSI são propostas de gestão desta revisão, e não prazos fixados pelo item 3.1.5 do Manual do Pró-Gestão.

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

SUMÁRIO

1. INTRODUÇÃO 4

2. OBJETIVOS E PRINCÍPIOS 4

3. APLICAÇÃO E ABRANGÊNCIA 5

4. RESPONSABILIDADES ESPECÍFICAS 6

5. MONITORAMENTO E REGRAS DE UTILIZAÇÃO 8

6. IDENTIFICAÇÃO E CONTROLE DE ACESSO LÓGICO 10

7. COMPUTADORES E RECURSOS TECNOLÓGICOS 11

8. PRIVACIDADE E PROTEÇÃO DAS INFORMAÇÕES 12

9. DISPOSITIVOS MÓVEIS E ACESSO REMOTO 13

10. SEGURANÇA FÍSICA DAS INSTALAÇÕES 13

11. BACKUP, RESTAURAÇÃO E CONTINGÊNCIA 14

12. INCIDENTES, VIOLAÇÕES E CONSCIENTIZAÇÃO 16

13. DISPOSIÇÕES FINAIS 17

ANEXO I – TERMO DE CIÊNCIA E COMPROMISSO 18

ANEXO II – IMPLANTAÇÃO E COMPATIBILIZAÇÃO 19

REFERÊNCIAS DA REVISÃO 21

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial

Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

1. INTRODUÇÃO

A Política de Segurança da Informação – PSI estabelece as regras institucionais para proteção das informações e utilização dos recursos do Guaratuba Previdência – GUARAPREV, em meio físico ou digital. Sua execução integra as atividades de gestão, prestação de serviços previdenciários e controle interno.

Esta revisão destina-se à consolidação da PSI instituída pela Portaria nº 006/2023, mediante nova deliberação e formalização. A substituição da versão anterior produzirá efeitos somente após a edição e publicação do ato competente, observadas as disposições do item 13.

A referência de certificação é o item 3.1.5 do Manual do Pró-Gestão RPPS, versão 4.2, para o Nível II: abrangência e responsabilidades, regras de uso de recursos, cópias de segurança dos sistemas e bancos de dados e controles de acesso físico e lógico, com contingência, mapeamento e manualização. [1]

A PSI define o que deve ser protegido e as obrigações a cumprir. O manual complementar descreve como executar, autorizar, conferir e registrar os controles, com os parâmetros de cada recurso. A aprovação desta Política não aprova automaticamente parâmetros pendentes ou versões incompatíveis do manual.

2. OBJETIVOS E PRINCÍPIOS

São objetivos desta Política preservar a continuidade das atividades, reduzir o risco de perda e de uso indevido de informações, organizar as responsabilidades e permitir a verificação dos controles e de seus resultados.

Confidencialidade: limitar o acesso às pessoas legitimadas e autorizadas, sem afastar as obrigações de transparência e de acesso à informação.

Integridade: preservar a exatidão e a completude das informações, dos registros e dos métodos de processamento, prevenindo alterações indevidas.

Disponibilidade: manter condições de acesso e recuperação compatíveis com as necessidades dos serviços e com os direitos dos interessados.

As medidas observarão finalidade institucional, necessidade, proporcionalidade, identificação dos responsáveis, rastreabilidade das ações e melhoria contínua, em consonância com a legislação aplicável. [2–4]

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

3. APLICAÇÃO E ABRANGÊNCIA

3.1 Pessoas abrangidas

Esta Política aplica-se aos dirigentes, servidores efetivos e comissionados, cedidos, temporários, estagiários, membros dos conselhos e do Comitê de Investimentos, prestadores e demais pessoas autorizadas que acessem informações ou recursos do GUARAPREV, independentemente do vínculo e do local da atividade.

Os fornecedores deverão observar as obrigações de segurança relacionadas aos serviços contratados. A Diretoria Executiva deverá providenciar sua previsão nos instrumentos pertinentes e tratar as adequações dos contratos existentes, sem presumir obrigações contratuais que ainda não tenham sido formalizadas.

3.2 Informações, equipamentos e sistemas

A abrangência compreende informações recebidas, produzidas, processadas ou custodiadas pelo GUARAPREV, inclusive em documentos físicos, computadores, servidor de arquivos, equipamento de armazenamento em rede (NAS), correio eletrônico, dispositivos móveis, sistemas e bancos de dados próprios ou administrados por terceiros.

A Diretoria Executiva, com os gestores e a TI, manterá relação atualizada dos recursos e dos dados institucionais, mediante a F-01, Partes B, C e D, ou registro equivalente. Para cada recurso serão identificados localização, administrador, responsável institucional, dados incluídos e excluídos dos controles, acessos, guarda, recuperação e limitações conhecidas.

A cobertura de um equipamento ou serviço não comprova a proteção dos demais. O backup do servidor de arquivos não será tratado como backup automático de documentos locais, caixas de e-mail ou bases de sistemas terceirizados. A proteção desses recursos deverá ser verificada individualmente.

3.3 Criticidade e complementação

Os gestores indicarão os serviços e as informações prioritários para a continuidade das atividades. A TI avaliará os controles e as condições de recuperação, registrando os parâmetros no manual. Ausência de informação será tratada como pendência de levantamento, e não como confirmação de cobertura ou de inexistência do controle.

A contratação ou entrada em operação de novo recurso deverá ser acompanhada da identificação de responsabilidades, proteção dos dados, acessos e recuperação. A desativação exigirá preservação das informações sujeitas à guarda e encerramento controlado dos acessos.

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

4. RESPONSABILIDADES ESPECÍFICAS

4.1 Conselho do GUARAPREV

Ao Conselho Administrativo, na condição de colegiado deliberativo, compete apreciar esta Política e suas revisões e acompanhar as providências institucionais que lhe forem submetidas, nos limites da legislação e do regimento. A deliberação será registrada em ata e formalizada pelo instrumento cabível. Esta Política não amplia competências legais nem atribui ao Conselho a execução de rotinas de TI. [2]

4.2 Diretoria Executiva

A Diretoria Executiva deverá encaminhar a Política à deliberação competente, promover sua formalização, publicação e aplicação, organizar os recursos necessários e acompanhar as adequações. Deverá formalizar a área ou o prestador responsável pela execução técnica e indicar o responsável institucional pelo acompanhamento, seus substitutos e as competências de autorização.

Caberá à Diretoria aprovar os parâmetros e procedimentos operacionais dentro de sua competência, após manifestação técnica, e encaminhar ao órgão competente as matérias que exijam deliberação superior. A manutenção da PSI e dos controles não poderá ficar atribuída genericamente a departamento não identificado.

4.3 Responsável institucional

O responsável institucional articulará a atuação dos gestores, da TI e dos fornecedores, manterá a identificação das versões e das evidências, acompanhará os registros e cobrará o tratamento das pendências. Não substitui o executor técnico, a autoridade competente ou o encarregado pelo tratamento de dados pessoais.

4.4 Gestores de pessoas e de processos

Os gestores deverão indicar a necessidade e o prazo dos acessos, encaminhar as autorizações competentes, comunicar movimentações e desligamentos sem demora, orientar as equipes e verificar a aplicação das regras em sua área. Deverão conferir a utilidade e a consistência das informações recuperadas e comunicar documentos ou serviços não abrangidos pelos controles.

A distribuição nominal das atribuições será registrada na F-01, Partes A e D. A autorização, a execução e a conferência deverão ser distinguíveis; eventual acúmulo de funções será documentado, com revisão por outro responsável competente, especialmente em alterações do próprio acesso.

A denominação “Conselho Administrativo” corresponde à Lei Complementar Municipal nº 015/2023. A formalização observará o regimento e eventuais alterações legais aplicáveis, a conferir na instrução do ato. Não se cria nova unidade administrativa ou comitê por esta PSI.

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

4. RESPONSABILIDADES ESPECÍFICAS

4.5 Área ou prestador de Tecnologia da Informação

A TI será responsável pela administração e execução técnica dos controles dos recursos sob sua gestão, conforme designação ou vínculo formal. Deverá configurar acessos, manter a proteção e as atualizações aplicáveis, executar e conferir backups, realizar testes, atuar na contingência e preservar os registros de suas ações.

Deverá informar à Diretoria e aos gestores as limitações, falhas, riscos residuais e necessidades de adequação. A capacidade de administrar um sistema não constitui autorização irrestrita para consultar informações pessoais, divulgar conteúdo ou alterar registros sem finalidade de serviço.

4.6 Fornecedores de sistemas e serviços

Os prestadores executarão os controles sob sua administração, no escopo formalizado, e deverão informar responsáveis e canais de atendimento, condições de backup e recuperação, controles de acesso e evidências disponibilizadas. Solicitações de criação, alteração e bloqueio de contas exigirão confirmação da execução.

Os acessos de suporte deverão ter titular identificável, finalidade, privilégio e período autorizados. A necessidade de continuidade do serviço não dispensa a proteção das credenciais. Os instrumentos contratuais deverão prever cooperação no tratamento de incidentes, comunicação sem demora injustificada e preservação ou devolução dos dados ao término do serviço.

4.7 Guarda física, proteção de dados e controle interno

O responsável pela guarda controlará ambientes, chaves, visitantes e movimentações de documentos. O encarregado pelo tratamento de dados pessoais e a assessoria jurídica atuarão em suas atribuições, especialmente quanto a direitos dos titulares, incidentes e comunicações. As instâncias de controle interno acompanharão as evidências e recomendações dentro de suas competências, sem substituir a execução dos controles.

4.8 Usuários

Cada usuário deverá conhecer e cumprir a PSI, utilizar apenas os recursos e acessos autorizados, proteger suas credenciais, armazenar documentos nos locais institucionais definidos e comunicar imediatamente falhas, perdas e suspeitas de uso indevido. Deverá colaborar com os testes e com a devolução dos recursos ao término da necessidade de uso.

A ciência da Política será registrada no ingresso, em suas revisões e sempre que necessário. O dever de proteção de informação legalmente restrita permanece após o desligamento, sem impedir o cumprimento de obrigações legais ou comunicações legítimas às autoridades.

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

5. MONITORAMENTO E REGRAS DE UTILIZAÇÃO

5.1 Monitoramento e auditoria do ambiente

O GUARAPREV poderá monitorar os recursos institucionais para proteger serviços, prevenir acessos indevidos e apurar ocorrências, com finalidade definida, extensão necessária e acesso restrito aos responsáveis. Os usuários serão informados das regras de monitoramento, sem prejuízo das diligências legalmente cabíveis.

Os registros deverão permitir, conforme a capacidade do recurso, identificar quem realizou a ação, o recurso afetado, a data, o horário e o resultado. Sua proteção, retenção, consulta e descarte serão definidos no manual, observadas as obrigações legais e de preservação de evidências. É vedada a alteração ou eliminação de registros para ocultar ações.

As informações de monitoramento não serão tornadas públicas apenas por solicitação de dirigente. Seu acesso ou compartilhamento dependerá de finalidade, competência e fundamento jurídico adequados, distinguindo-se uso interno autorizado de divulgação pública. O monitoramento não afasta a proteção de dados pessoais e da intimidade. [3–4]

5.2 Correio eletrônico institucional

O e-mail institucional destina-se às atividades do GUARAPREV. O uso pessoal eventual não poderá prejudicar o serviço, gerar custo ou risco relevante, envolver atividade vedada ou substituir contas particulares para cadastros pessoais e redes sociais.

São vedados o envio de mensagens ilícitas, discriminatórias, ofensivas ou de propaganda político-partidária; a falsificação de remetente; o uso de conta sem autorização; a distribuição não autorizada em massa; a divulgação indevida de dados; e a abertura ou o envio de conteúdo suspeito sem avaliação adequada.

O usuário deverá conferir destinatários, anexos e legitimidade de pedidos de dados ou pagamentos. Mensagens suspeitas deverão ser encaminhadas pelo canal de atendimento definido, sem fornecer credenciais. Mensagens sujeitas à guarda ou investigação não poderão ser eliminadas para impedir sua recuperação.

O provedor, as caixas institucionais, os administradores, a retenção e a recuperação serão identificados por serviço. Caixas de uso setorial deverão, sempre que suportado, operar por delegação a usuários individualizados, sem compartilhamento de senhas pessoais. Limitações de anexos e meios seguros de transferência serão definidos pela TI, sem impedir o uso legítimo de criptografia.

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

5. MONITORAMENTO E REGRAS DE UTILIZAÇÃO

5.3 Internet e serviços de comunicação

A internet e os serviços de comunicação serão utilizados prioritariamente para as atividades institucionais. O uso eventual de notícias e serviços pessoais deverá respeitar as restrições da PSI, o desempenho dos sistemas e as atribuições funcionais.

É vedado contornar controles de segurança; obter ou tentar acesso não autorizado; instalar ou distribuir software irregular; propagar código malicioso; executar serviços de compartilhamento não autorizados; praticar assédio; ou divulgar informações protegidas em redes sociais, aplicativos, repositórios particulares ou serviços não autorizados.

Programas, aplicativos e extensões somente serão instalados ou alterados mediante autorização e avaliação técnica, com licenciamento aplicável. Os meios de transferência e armazenamento externo de dados institucionais dependerão de autorização e proteção compatível. Somente pessoa autorizada poderá manifestar-se oficialmente em nome do GUARAPREV.

5.4 Acesso a informações em meio físico

Os documentos e ambientes que contenham informações protegidas terão acesso limitado às pessoas autorizadas. A consulta, a reprodução e a retirada interna serão registradas conforme POP-SI-04 e F-05 ou protocolo equivalente, contendo solicitante, autorizador quando exigido, responsável pela guarda, documento, finalidade, datas e horários de movimentação e devolução.

O responsável pela guarda conferirá integridade, organização e completude na devolução, registrando ausência, dano ou outra divergência. Não será permitido retirar folhas, efetuar alterações indevidas ou registrar como devolvido documento não recebido. Cópias e reproduções deverão respeitar a autorização e as restrições legais.

O procedimento ordinário de retirada é interno. A remessa externa de documento protegido somente poderá ocorrer em hipótese legal ou determinação competente, mediante autorização formal, protocolo de custódia e proteção do transporte. Essa hipótese deverá receber instrução específica e não se confunde com a retirada interna descrita no manual.

Os controles físicos não impedirão o exercício regular de direitos pelos interessados nem o atendimento às autoridades. A forma de acesso será compatibilizada com a Lei de Acesso à Informação e com a proteção de dados pessoais. [3–4]

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

6. IDENTIFICAÇÃO E CONTROLE DE ACESSO LÓGICO

6.1 Identificação, autorização e encerramento

Os acessos de pessoas serão individuais, identificáveis e limitados ao necessário para a função. É vedado compartilhar contas ou senhas pessoais, inclusive administrativas, certificados e demais meios de identificação individual. Uma solicitação do próprio interessado não substitui a autorização competente.

Concessões e alterações exigirão solicitação, justificativa, perfil, prazo quando aplicável, autorização, execução e conferência, registrados no F-04 ou sistema equivalente. A TI executará os recursos sob sua gestão; para os demais, o administrador do serviço deverá confirmar a execução. O cadastro deverá distinguir contas comuns, administrativas e técnicas.

Os acessos serão bloqueados ou revogados sem demora quando cessar sua necessidade, no desligamento, na mudança de função ou em medida de contenção. O gestor comunicará o fato tempestivamente; o responsável acompanhará a efetivação em todos os recursos atingidos. O envio do pedido ao fornecedor não comprova bloqueio concluído.

6.2 Credenciais e privilégios

Credenciais iniciais e senhas padrão deverão ser alteradas antes do uso regular, quando aplicável. Recuperações de senha exigirão verificação de identidade e canal seguro. É vedado registrar senhas em formulários de controle, mensagens desprotegidas ou arquivos de texto acessíveis; sua guarda técnica utilizará meio protegido e autorizado.

Contas administrativas terão titular, finalidade e privilégios definidos, uso limitado às tarefas autorizadas e registro das intervenções. A conferência das alterações do próprio acesso será realizada por outro responsável competente. Os privilégios serão revistos periodicamente, segundo calendário registrado na F-01, e nas mudanças de vínculo ou atribuição.

Deverá ser utilizada autenticação multifator nos acessos administrativos e remotos quando disponibilizada pelo serviço. Limitações técnicas deverão ser registradas, com medidas de proteção alternativas e providência de adequação aprovada, sem serem tratadas como controle já implantado.

6.3 Contas técnicas e serviços de terceiros

Contas técnicas destinadas à execução automática de serviços terão finalidade, responsável pela custódia e permissões documentados. Não servirão de conta coletiva para uso pessoal. Necessidades de intervenção humana deverão preservar a identificação de quem atuou, mediante procedimento autorizado e registro, sem liberar o compartilhamento de login administrativo.

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

7. COMPUTADORES E RECURSOS TECNOLÓGICOS

7.1 Uso e manutenção

Os equipamentos e sistemas institucionais serão utilizados conforme sua finalidade e as orientações técnicas. Instalações, manutenção, mudança de configuração ou conexão de dispositivos dependerão de autorização e acompanhamento da TI ou de prestador habilitado. Alterações relevantes deverão ser registradas e considerar seus efeitos na recuperação do serviço.

A TI manterá os mecanismos de proteção e as atualizações compatíveis com o recurso e sua criticidade. Componentes sem suporte ou limitações de atualização deverão ser registrados para tratamento, com proteção compensatória e encaminhamento. Usuários não poderão desativar controles nem executar testes ou comandos que comprometam o serviço sem autorização.

Os terminais deverão permanecer bloqueados quando não utilizados. Dispositivos desconhecidos, mensagens suspeitas ou comportamento anormal deverão ser comunicados. O acesso a equipamentos por suporte remoto observará identificação, autorização, necessidade e registro da intervenção.

7.2 Armazenamento e proteção de documentos

Os documentos necessários às atividades deverão ser mantidos nos repositórios institucionais indicados pela TI e pelos gestores, com cobertura de backup identificada. A utilização de pasta de rede, por si só, não comprova sua inclusão na cópia: o escopo deverá constar da F-01.

Documentos institucionais mantidos apenas em computadores ou dispositivos locais deverão ser identificados e transferidos para local protegido ou incluídos em solução de backup validada. Antes de excluir a origem, deverão ser conferidos o conteúdo, a integridade e o acesso no destino. A existência de arquivos locais não autoriza atribuir automaticamente ao usuário toda responsabilidade por eventual perda.

Arquivos particulares ou estranhos ao serviço não deverão ocupar os repositórios institucionais. Sua regularização observará orientação ao usuário, finalidade e registro, sem eliminar documentos sujeitos à guarda, direitos de terceiros ou evidências de ocorrência.

7.3 Reutilização, devolução e descarte

A transferência, manutenção externa, reutilização ou descarte de equipamento ou mídia exigirá verificação dos dados existentes, preservação do que deve ser guardado e eliminação segura do que puder ser descartado. A devolução de recursos e o encerramento de acessos serão registrados, sem perda indevida de informações institucionais.

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

8. PRIVACIDADE E PROTEÇÃO DAS INFORMAÇÕES

8.1 Finalidade e acesso legítimo

O tratamento de dados pessoais observará a finalidade pública e a base legal aplicável, com utilização apenas dos dados necessários e controles proporcionais aos riscos. Dados de segurados, beneficiários, servidores e terceiros não serão utilizados para finalidade particular ou incompatível com a atividade institucional. [3]

A autorização administrativa para acessar ou compartilhar dados não substitui o fundamento jurídico do tratamento. O acesso será limitado às pessoas que necessitem das informações para o serviço e será objeto de registro e proteção compatíveis. O conhecimento técnico ou funcional de uma informação não permite sua divulgação irrestrita.

8.2 Transparência, direitos e compartilhamento

O caráter institucional da informação não a torna automaticamente sigilosa. A disponibilização ao público, aos titulares e às autoridades observará a legislação, distinguindo informação de acesso público, dados pessoais protegidos e hipóteses legais de restrição. As solicitações serão encaminhadas aos canais e responsáveis competentes. [3–4]

O compartilhamento com prestadores deverá se limitar ao necessário ao serviço e estar amparado pelo instrumento e pela base jurídica pertinentes. Deverão ser definidas instruções de tratamento, acesso, confidencialidade, segurança, comunicação de incidentes, guarda e devolução ou eliminação ao término da necessidade, respeitadas as obrigações legais.

8.3 Guarda e eliminação

Os prazos de guarda dos documentos e registros observarão sua finalidade, a legislação, os instrumentos de gestão documental aplicáveis e eventuais impedimentos de eliminação por investigação, processo ou obrigação de preservação. O prazo de retenção de uma cópia de backup não substitui a obrigação de guarda do documento original.

A eliminação deverá ser autorizada e registrada, quando cabível, e impedir a recuperação indevida da informação descartada. Documentos em papel, mídias e arquivos digitais terão tratamento compatível com sua natureza e restrição de acesso.

8.4 Atuação institucional

Dúvidas sobre base legal, atendimento a titulares ou comunicação de incidentes serão submetidas ao encarregado pelo tratamento de dados pessoais e à assessoria jurídica, segundo suas atribuições. A Diretoria assegurará a articulação com a TI e os gestores. O Termo de Ciência desta PSI não equivale a consentimento genérico para tratamento de dados nem a renúncia de direitos.

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

9. DISPOSITIVOS MÓVEIS E ACESSO REMOTO

O uso de notebooks, smartphones, mídias removíveis ou outros dispositivos para dados institucionais dependerá de autorização e identificação do responsável. Os controles deverão contemplar bloqueio de acesso, configurações seguras, proteção do transporte e armazenamento e inclusão dos dados na rotina de guarda e recuperação pertinente.

Documentos e cópias não deverão ficar exclusivamente no dispositivo móvel nem ser mantidos junto dele quando isso comprometer a recuperação. O usuário utilizará os repositórios e procedimentos definidos pela TI, sem recorrer a contas pessoais ou serviços não autorizados para armazenar dados institucionais.

O acesso remoto deverá utilizar meio autorizado e protegido, com identificação do usuário, perfil necessário e encerramento das sessões. Acesso de suporte de terceiro será restrito ao serviço e ao período autorizado. Perda, furto, roubo ou suspeita de comprometimento será comunicada imediatamente à TI e ao gestor para contenção e avaliação.

Quando houver dispositivo particular autorizado, as condições de uso e suporte deverão ser formalizadas, limitando a intervenção institucional ao necessário à proteção do serviço e dos dados. Esta PSI não autoriza inspeção indiscriminada de conteúdo particular.

10. SEGURANÇA FÍSICA DAS INSTALAÇÕES

As salas, armários e demais ambientes que abriguem servidor de arquivos, NAS, equipamentos de rede, mídias e documentos protegidos terão responsáveis e controles de acesso definidos conforme a estrutura existente. Não se pressupõe datacenter próprio.

As chaves e credenciais físicas serão controladas, e terceiros somente ingressarão com autorização e acompanhamento quando exigido. A perda de chave ou suspeita de acesso indevido será comunicada para avaliação e substituição do mecanismo de acesso, quando necessária.

Os equipamentos deverão ser protegidos contra acesso indevido, remoção, água, calor e outras condições incompatíveis com seu funcionamento, observadas as orientações técnicas do fabricante. Os ambientes serão mantidos organizados, sem alimentos, líquidos ou materiais que ofereçam risco aos recursos.

A guarda de uma cópia no mesmo local do servidor não será tratada como proteção suficiente contra a indisponibilidade integral da unidade. A proteção física e a estratégia de recuperação serão compatibilizadas com a segunda fonte prevista no item 11 e com o POP-SI-04.

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

11. BACKUP, RESTAURAÇÃO E CONTINGÊNCIA

11.1 Cobertura e parâmetros

Deverão existir cópias de segurança dos sistemas informatizados, bancos de dados e informações necessários à continuidade das atividades. A cobertura incluirá os componentes necessários à recuperação, identificados pela TI ou pelo prestador, e não apenas arquivos avulsos desvinculados do funcionamento do serviço.

Para cada recurso, a F-01 deverá identificar dados incluídos e excluídos, modalidade, frequência, agendamento, destino, retenção, capacidade, executor, conferente e condições de restauração. Em cópias incrementais, deverão ser preservados e verificados os componentes e a sequência necessários à recuperação.

Sistemas e e-mails administrados por terceiros terão condições de cópia, retenção, recuperação e fornecimento de evidências formalizadas e verificadas. Uma declaração genérica de que o fornecedor realiza backup não substituirá a identificação de cobertura e de como solicitar e validar a recuperação.

11.2 Execução, conferência e proteção

As rotinas deverão ser automatizadas, com programação adequada ao uso do serviço. Exceções técnicas serão justificadas e acompanhadas, sem interrupção indevida das cópias existentes. Cada execução deverá ter resultado conferido, evidência identificada e tratamento de falhas, no F-02 ou registro equivalente.

As cópias serão protegidas contra leitura, alteração e eliminação não autorizadas, com controle de privilégios e armazenamento adequado. A TI avaliará meios de impedir que o comprometimento do ambiente principal alcance simultaneamente todas as cópias, considerando segregação de acessos e cópias isoladas ou imutáveis, conforme a solução adotada.

11.3 Segunda fonte em local distinto

Os dados abrangidos pela rotina de backup deverão contar com segunda fonte de cópia em local fisicamente distinto da unidade principal, apta a apoiar a recuperação quando esta ficar indisponível. A solução poderá ser própria ou contratada, sem imposição de tecnologia ou fornecedor específico, e deverá ter proteção de acesso e capacidade de restauração verificadas.

O NAS na mesma unidade não substitui essa segunda fonte. A implantação ou adequação deverá ser tratada no plano do item 13, com solução, responsável e prazo. Enquanto não concluída, a limitação permanecerá registrada e acompanhada, sem declaração de proteção adicional existente ou de atendimento integral.

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

11. BACKUP, RESTAURAÇÃO E CONTINGÊNCIA

11.4 Testes de restauração

A TI e os gestores estabelecerão calendário de testes de restauração, com periodicidade definida conforme a criticidade do recurso e registrada na F-01. O calendário deverá ser aprovado e identificar amostra, ambiente, executor e responsável pela validação. Cada recurso deverá ter intervalo expresso e calendário de execução, sem periodicidade indefinida.

O teste deverá demonstrar a recuperação e a utilização das informações ou do sistema, em ambiente seguro, evitando sobrescrever produção sem autorização. Serão registrados cópia e componentes utilizados, início, término, verificações, resultado técnico, conferência funcional e eventuais falhas, por meio do F-03 ou registro equivalente.

A conclusão de uma tarefa de backup sem mensagem de erro não comprova restauração. Falhas de cópia ou de teste deverão ser corrigidas, com reexecução no primeiro momento seguro disponível e acompanhamento até validação. Mudança relevante de ambiente, ferramenta ou estratégia e falha que afete a recuperação exigirão avaliação de teste adicional.

11.5 Contingência e recuperação das atividades

O POP-SI-02 deverá contemplar comunicação por canal principal e alternativo, identificação dos serviços afetados, diagnóstico, preservação de evidências, contenção, acionamento de prestadores e avaliação de cópia utilizável ou alternativa segura. Deverá abranger a hipótese de indisponibilidade da unidade e de inacessibilidade do servidor e do NAS locais.

A autorização de recuperação, a execução técnica, a validação dos dados e a liberação de retomada serão identificadas na F-01. A TI e os gestores definirão a prioridade dos serviços e os objetivos de tempo de recuperação e de perda de dados tolerável, compatíveis com o ambiente e os riscos, sem presumir recuperação imediata ou perda zero.

O restabelecimento dependerá de teste do funcionamento e da consistência das informações. A ausência de cópia utilizável ou a recuperação parcial deverá permanecer registrada, com responsável, próxima ação e comunicação aos afetados. Alternativas temporárias dependerão de autorização, controle e posterior recomposição das informações.

Os procedimentos de backup, recuperação e acesso permanecerão mapeados e manualizados nos POP-SI-01 a POP-SI-04. Os registros deverão permitir distinguir falha operacional, pendência estrutural, teste programado e incidente. A conclusão técnica não dispensa providências de proteção de dados ou de apuração.

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

12. INCIDENTES, VIOLAÇÕES E CONSCIENTIZAÇÃO

12.1 Comunicação e tratamento

Falha relevante, perda de equipamento ou documento, acesso indevido, vazamento ou suspeita de comprometimento deverá ser comunicada imediatamente à TI e ao responsável institucional, pelos canais definidos. Não se aguardará confirmação completa do dano para registrar e avaliar a ocorrência.

A TI adotará a contenção tecnicamente adequada, preservará as evidências e manterá registro de decisões e intervenções. Medidas urgentes previstas no procedimento e nas competências formalizadas não dependerão de reunião prévia do Conselho. Quando envolver dados pessoais, a Diretoria acionará o encarregado e o apoio jurídico para avaliação e comunicações cabíveis.

12.2 Incidentes envolvendo dados pessoais

Quando o incidente puder acarretar risco ou dano relevante aos titulares, caberá ao controlador comunicar à ANPD e aos titulares, na forma do art. 48 da LGPD e da Resolução CD/ANPD nº 15/2024. O prazo aplicável é de três dias úteis, contado do conhecimento pelo controlador de que o incidente afetou dados pessoais, ressalvado prazo de legislação específica ou norma superveniente. [3, 5]

A avaliação e as comunicações não dependerão do término da investigação ou de aprovação posterior do Conselho. A complementação de informações observará o regulamento. O fornecedor deverá informar o incidente sem demora injustificada e cooperar com o controlador, sem substituí-lo em suas obrigações legais.

Serão mantidos registros dos incidentes, inclusive dos não comunicados externamente, com justificativa da avaliação, medidas e responsáveis, observadas as regras de conservação do art. 10 do regulamento e as particularidades da gestão documental pública. Dados e evidências terão acesso restrito à finalidade de tratamento.

12.3 Apuração e conscientização

O descumprimento será apurado pela autoridade competente conforme o vínculo e a legislação ou contrato aplicável, com o procedimento e as garantias pertinentes. Não se presumem culpa, responsabilidade integral por todo dano ou aplicação automática de penalidade. O bloqueio preventivo de acesso é medida de proteção, não punição disciplinar aplicada pela TI.

Serão realizadas orientações de segurança no ingresso, nas revisões da PSI e conforme os riscos identificados, com registro da ciência. Incidentes podem decorrer de falhas técnicas, erro ou ação de terceiros; seu relato de boa-fé deverá ser estimulado para permitir correção e prevenção.

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

13. DISPOSIÇÕES FINAIS

13.1 Aprovação, formalização e publicação

A revisão será submetida à validação técnica e à apreciação do Conselho, observadas as competências locais e a análise jurídica do ato. A aprovação será registrada em ata e no instrumento cabível. A vigência será definida no ato de instituição, após a publicação exigida, com disponibilização da PSI aprovada na internet. [1–2]

O ato de instituição deverá identificar expressamente a substituição da PSI vinculada à Portaria nº 006/2023 e tratar sua revogação ou alteração pela autoridade competente, bem como eventuais atos posteriores. Até a eficácia do novo ato, esta minuta não revoga normas nem autoriza afastar controles vigentes.

13.2 Implantação e compatibilização

Em até 30 dias da vigência, a Diretoria Executiva deverá apresentar plano de adequação, com a TI e os gestores, contendo responsáveis e substitutos, levantamento dos recursos, situação dos controles, parâmetros a concluir, compatibilização do manual, segunda fonte de cópia, medidas de proteção, prazos e recursos necessários. A execução observará as competências de aprovação e contratação.

O acompanhamento será trimestral até a conclusão do plano, com registro das providências e comunicação ao Conselho das pendências relevantes. Medidas urgentes não aguardarão o encerramento do prazo do plano. Os controles existentes deverão ser mantidos, e limitações temporárias exigirão tratamento documentado, sem dispensar obrigação legal nem comprovar atendimento de requisito não implantado.

O manual, seus fluxogramas e fichas deverão ser compatibilizados com esta versão antes da adoção operacional definitiva. A aprovação da PSI não certifica, por si, a execução das rotinas ou o atendimento integral ao Pró-Gestão. O Anexo II identifica a situação informada e os principais pontos de compatibilização.

13.3 Ciência, revisão e guarda

A Diretoria promoverá a divulgação e a ciência das pessoas abrangidas, com registro conforme Anexo I ou meio equivalente. Detalhes técnicos sensíveis, credenciais e registros nominais não integrarão a versão pública da PSI; sua guarda e disponibilização observarão finalidade e fundamento legal.

A necessidade de revisão será avaliada anualmente e sempre que houver alteração relevante de ambiente, serviços, legislação, riscos ou estrutura. Alterações normativas da PSI serão submetidas à aprovação competente. Ajustes de parâmetros do manual serão formalizados pela autoridade responsável, desde que não reduzam nem contrariem as regras desta Política.

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

ANEXO I – TERMO DE CIÊNCIA E COMPROMISSO

Política de Segurança da Informação – PSI do GUARAPREV

Identificação	Preenchimento
Nome completo	_____
Vínculo / cargo / função	_____
Matrícula, se houver	_____
Unidade / empresa	_____
Versão da PSI e ato de instituição	_____
Recebimento da PSI (data)	____/____/_____

Declaro que recebi ou tive acesso à versão da Política de Segurança da Informação identificada acima e que fui informado(a) sobre os procedimentos aplicáveis às atividades que desempenho junto ao GUARAPREV.

Comprometo-me a utilizar os recursos e informações para as finalidades autorizadas, proteger as credenciais sob minha guarda, observar os controles de acesso e armazenamento e comunicar falhas, perdas ou suspeitas de incidente pelos canais institucionais divulgados.

Declaro estar ciente das regras de monitoramento para fins de segurança e de que o tratamento de dados e registros deve respeitar os limites legais e as finalidades informadas. Em caso de dúvida, buscarei orientação do gestor, da TI ou do responsável institucional.

Resguardarei informações legalmente protegidas mesmo após o término do vínculo, sem prejuízo do cumprimento de obrigações legais, do exercício de direitos ou de comunicações legítimas às autoridades.

Este Termo não constitui consentimento genérico para tratamento de dados pessoais, renúncia a direitos ou assunção automática de responsabilidade por quaisquer danos. Eventual descumprimento será apurado conforme a legislação e o vínculo aplicáveis.

Guaratuba/PR, _____ de _____ de _____.

_____

Assinatura da pessoa que declara

Registro da ciência: assinatura física, eletrônica ou outro meio institucional que permita identificar a pessoa, a versão recebida e a data. O Termo será guardado em registro institucional de acesso controlado.

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

ANEXO II – IMPLANTAÇÃO E COMPATIBILIZAÇÃO

A. Situação informada e providências

A manifestação da TI encaminhada para esta revisão informa backup incremental diário do servidor de arquivos para um NAS instalado no próprio GUARAPREV, na mesma unidade. Esse registro descreve o relato recebido, não uma auditoria da execução nem a cobertura de todos os recursos. [7–8]

Tema	Providência de implantação ou confirmação
Recursos e dados	Completar a relação nominal de servidor, NAS, estações, documentos locais, e-mails, sistemas e fornecedores. Identificar cobertura, exclusões e proteção por recurso.
Backup existente	Confirmar pastas, ferramenta, tarefa, componentes da cópia incremental, retenção, capacidade, executor e conferente. Vincular evidências reais às fichas.
Segunda fonte	Confirmar existência; se ausente ou insuficiente, definir e implantar solução em local distinto, com proteção de acesso e teste, nos termos do plano aprovado.
Restauração e contingência	Aprovar calendário de testes, prioridades, responsáveis, canais e condições de recuperação, inclusive quando a unidade e a cópia local estiverem indisponíveis.
Acessos e prestadores	Identificar administradores, contas, perfis, autorizadores, executores e conferentes. Obter confirmações dos serviços terceirizados e tratar limitações contratuais.
Responsabilidades e ciência	Formalizar responsáveis e substitutos; divulgar canais; dar ciência da PSI e do manual compatibilizado; organizar registros e acompanhamento.

B. Vinculação dos registros

As providências serão registradas na F-01, Partes A a D, ou em plano equivalente, sem duplicar formulários desnecessariamente. Cada pendência terá situação, medida, responsável, prazo, evidência esperada e data de conferência. F-02 a F-05 permanecerão destinados aos registros de execução dos respectivos processos.

A relação acima orienta a implantação. Não confirma tecnologia, retenção, calendário, prestador ou responsável ainda não informado. O preenchimento de uma ficha não substitui evidência de execução nem encerra pendência sem verificação.

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

ANEXO II – IMPLANTAÇÃO E COMPATIBILIZAÇÃO

C. Ajustes de referência do manual – versão 1.1

Antes da adoção definitiva, o manual revisado deverá receber a identificação desta PSI, do ato e da data de vigência, com registro de nova revisão e validação dos pontos abaixo. Preservam-se o espelho institucional e os códigos dos processos e formulários. [7]

Passagem do manual 1.1	Compatibilização necessária
Itens 2.3, 2.4 e 2.8; referências da PSI	Substituir referências à minuta sem ato e à alternativa de testes de 90 ou 120 dias pela PSI instituída e pelo calendário técnico aprovado. Registrar o ato de substituição da Portaria nº 006/2023.
Itens 2.6 e 2.8; POP-SI-01; F-01 e F-02	Relacionar a rotina local informada com a obrigação de segunda fonte em local distinto. Manter separadas evidência do backup local, situação da segunda fonte e providências do plano.
Item 2.7; POP-SI-03; F-04	Eliminar a referência à inconsistência não resolvida sobre logins compartilhados. Aplicar as regras da nova PSI para contas individuais, administrativas, técnicas, acessos remotos e autenticação.
POP-SI-02; F-03	Relacionar os canais e responsáveis pelo tratamento de dados pessoais ao item 12 desta PSI. Incorporar o controle das comunicações legais e da preservação de registros, sem exigir reunião do Conselho para medidas urgentes.
POP-SI-04; F-05	Manter o fluxo de retirada interna. Distinguir remessa externa por hipótese legal ou determinação competente, que depende de autorização e instrução específica de custódia.
Item 5; F-01; quadro de validação	Atualizar responsáveis, parâmetros, estado das pendências, aprovação e ciência. Não converter a aprovação da Política em declaração de implantação integral dos procedimentos.

As demais regras deverão ser conferidas pelos executores e gestores. Divergências materiais serão corrigidas formalmente, sem alterar a PSI por simples preenchimento de formulário. O encerramento da compatibilização exige versão identificada, validação e aprovação pelas instâncias competentes.

Este quadro é uma orientação de consolidação e não modifica, por si, o arquivo do manual versão 1.1. A proposta de nova PSI deve ser apreciada conjuntamente com seus efeitos nos procedimentos.

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

REFERÊNCIAS DA REVISÃO

[1] Ministério da Previdência Social. Manual do Pró-Gestão RPPS, versão 4.2, item 3.1.5, páginas 27–28. Referência específica de certificação para o Nível II. Fonte oficial.

[2] Município de Guaratuba. Lei Complementar nº 015, de 28 de fevereiro de 2023. Denominação da unidade gestora, organização institucional, competências e publicidade dos atos, especialmente arts. 3º, 75, 77 e 84. Fonte oficial.

[3] Brasil. Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais, especialmente princípios, tratamento pelo Poder Público e segurança dos dados, inclusive arts. 6º, 23 e 46 a 49. Fonte oficial.

[4] Brasil. Lei nº 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação, inclusive as disposições sobre proteção de informações pessoais. Fonte oficial.

[5] ANPD. Resolução CD/ANPD nº 15, de 24 de abril de 2024 – Regulamento de Comunicação de Incidente de Segurança. Orientações oficiais sobre comunicação, prazos e atuação de controladores e operadores. Fonte oficial.

[6] GUARAPREV. Portaria nº 006, de 06 de outubro de 2023, e PSI anexa, publicadas no Diário Oficial do Município de Guaratuba, edição nº 1029, páginas 12–17, disponibilizadas no portal institucional. Referência anterior objeto da proposta de consolidação. Fonte oficial.

[7] GUARAPREV. Manual de Padronização dos Processos de Segurança da Informação, versão 1.1, de 13 de outubro de 2026, apresentado nesta revisão. Documento operacional sujeito à validação e à compatibilização indicadas no Anexo II.

Fontes oficiais consultadas em 13/10/2026. As fontes normativas orientam a revisão; o relato da TI identifica somente a estrutura informada. Os detalhamentos institucionais e prazos de gestão propostos dependem da aprovação e das providências descritas nesta minuta.

_____

Rui Sergio Jacubovski

Presidente do Conselho Deliberativo do GUARAPREV

_____ _____

Roberto Mauro Lima Jaci Delmar Loeblein

_____ _____

Adriano Cavalheiro Petroski Ido Hepp

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial

Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000

Marcio Sakajiri Tarran

Diego Elickar

Tania Malinoski

Flavia Clara Savelli

+55 41 3472-8740 guaraprev@guaraprev.pr.gov.br guaraprevoficial
Rua José Bonifácio, 367 - Centro-Guaratuba/PR | 83.280-000