

Política de Segurança da Informação (PSI)

IPREV Jaguariaíva

1. APRESENTAÇÃO

O Instituto de Previdência dos Servidores Públicos Municipais de Jaguariaíva – IPREV, no exercício de suas competências institucionais, estabelece a presente Política de Segurança da Informação – PSI, com a finalidade de estabelecer princípios, diretrizes, responsabilidades e controles destinados à proteção das informações sob sua responsabilidade.

O IPREV realiza o tratamento de informações relacionadas a servidores ativos, aposentados, pensionistas, beneficiários, fornecedores, prestadores de serviços e demais pessoas que mantenham relação com a instituição. Esta política deverá ser observada por todos que tenham acesso a informações, sistemas, equipamentos ou recursos tecnológicos do IPREV.

2. CONCEITO CID

A Segurança da Informação será orientada pelo modelo CID (Confidencialidade, Integridade e Disponibilidade):

Confidencialidade - As informações devem ser acessadas somente por pessoas autorizadas e na medida necessária ao desempenho de suas atribuições.

Integridade - As informações devem permanecer corretas, completas, confiáveis e protegidas contra alterações indevidas.

Disponibilidade - As informações e sistemas necessários ao funcionamento do IPREV devem estar disponíveis aos usuários autorizados sempre que necessários.

A proteção adequada da informação exige equilíbrio entre os três princípios, pois uma informação excessivamente protegida, mas indisponível quando necessária, pode comprometer a prestação do serviço público. Da mesma forma, uma informação disponível a qualquer pessoa, mas sem controle de integridade ou confidencialidade, pode gerar graves riscos à instituição e aos segurados.

3. DEFINIÇÕES

Para fins desta Política:

Ativo de informação: recurso utilizado para produzir, armazenar, processar ou transmitir informação.

Usuário: pessoa autorizada a utilizar sistemas ou recursos do IPREV.

Incidente de segurança: evento que comprometa ou possa comprometer a confidencialidade, integridade ou disponibilidade das informações.

Backup: cópia de segurança de dados ou informações.

Acesso: possibilidade de consultar, utilizar, alterar ou administrar informação ou sistema.

Controle: medida destinada a reduzir determinado risco.

Risco: possibilidade de ocorrência de evento capaz de causar impacto negativo aos objetivos da instituição.

Dados pessoais: informação relacionada a pessoa natural identificada ou identificável.

Informação pública: informação cujo acesso não esteja legalmente restringido.

Informação restrita: informação cujo acesso deve ser limitado em razão de necessidade funcional, proteção de dados, segurança ou outra fundamentação legítima.

4. ABRANGÊNCIA

Esta Política de Segurança da Informação aplica-se obrigatoriamente a todos os servidores públicos e prestadores de serviços que acessem os sistemas e dados do RPPS. Os servidores têm o dever de utilizar as informações exclusivamente no exercício de suas funções, garantindo o sigilo, a confidencialidade e o manuseio adequado de dados sensíveis. Cabe aos prestadores de serviços cumprir rigorosamente as normas de segurança do RPPS, assegurando a proteção dos ativos e a integridade do ambiente tecnológico contratado.

É expressamente proibido o compartilhamento de credenciais de acesso, sendo a senha de uso pessoal, intransferível e de responsabilidade individual. Todo incidente de segurança, suspeita de vazamento ou uso indevido da informação deve ser imediatamente comunicado à equipe responsável pela gestão de TI. O não cumprimento destas diretrizes sujeitará os infratores às sanções administrativas, civis e penais cabíveis, conforme prevê a legislação vigente.

5. CONTROLE DE ACESSO

O acesso aos sistemas deverá obedecer ao princípio do menor privilégio, sendo concedido somente o nível necessário para o exercício das funções.

Deverão ser observadas as seguintes regras:

- I – Cada usuário deverá possuir identificação individual sempre que tecnicamente possível;
- II – Não deverá ocorrer compartilhamento de senhas;
- III – Os acessos deverão ser concedidos mediante autorização;
- IV – Os acessos deverão ser revistos periodicamente;

-
- V – Acessos deverão ser alterados quando houver mudança de função;
VI – Acessos deverão ser revogados quando cessar a necessidade;
VII – Contas de usuários desligados deverão ser desativadas;
VIII – Contas administrativas deverão ser restritas;
IX – Sempre que disponível, deverá ser utilizada autenticação multifator para acessos críticos.

6. SENHAS E AUTENTICAÇÃO

As senhas deverão:

- ser individuais;
- permanecer sob responsabilidade do usuário;
- não ser compartilhadas;
- não ser registradas em locais de fácil acesso por terceiros;
- possuir complexidade compatível com o sistema;
- ser alteradas quando houver suspeita de comprometimento.

Quando o sistema permitir, deverão ser utilizados recursos adicionais de autenticação.

7. USO ACEITÁVEL DOS RECURSOS TECNOLÓGICOS

Os equipamentos e sistemas do IPREV destinam-se prioritariamente ao desempenho das atividades institucionais.

É vedado:

- I – Instalar software não autorizado;
- II – Utilizar equipamentos institucionais para atividades ilícitas;
- III – Compartilhar credenciais;
- IV – Tentar acessar sistemas sem autorização;
- V – Remover mecanismos de segurança;
- VI – Armazenar informações institucionais em serviços pessoais sem autorização;
- VII – Utilizar recursos institucionais para causar danos a terceiros;
- VIII – Copiar informações institucionais para dispositivos não autorizados.

8. USO DE COMPUTADORES E DISPOSITIVOS MÓVEIS

Os usuários deverão:

- bloquear o equipamento ao se afastarem;
- manter os equipamentos protegidos;
- comunicar perda ou furto imediatamente;
- não deixar documentos confidenciais expostos;
- utilizar somente equipamentos autorizados para atividades institucionais;
- manter atualizações de segurança quando sob sua responsabilidade.

9. USO DA INTERNET

O acesso à internet deverá observar:

- I – Finalidade institucional;
- II – Legislação vigente;
- III – Segurança dos equipamentos;
- IV – Proteção das credenciais;
- V – Prevenção contra páginas maliciosas;
- VI – Proibição de downloads de arquivos suspeitos.

O usuário deverá evitar acessar links desconhecidos ou fornecer credenciais institucionais em páginas não confiáveis.

10. CORREIO ELETRÔNICO INSTITUCIONAL

O correio eletrônico institucional deverá ser utilizado para atividades relacionadas ao serviço.

O usuário deverá:

- verificar remetentes;
- evitar clicar em links suspeitos;
- não abrir anexos de origem duvidosa;
- não encaminhar informações restritas sem necessidade;
- conferir destinatários antes do envio;
- comunicar mensagens suspeitas.

11. ARMAZENAMENTO E COMPARTILHAMENTO

Informações institucionais deverão ser armazenadas preferencialmente em ambientes autorizados pelo IPREV.

O compartilhamento deverá observar:

- necessidade;
- autorização;
- classificação da informação;
- finalidade;
- segurança do meio utilizado.

Informações pessoais ou restritas não deverão ser compartilhadas por meios inadequados ou com pessoas sem necessidade de acesso.

12. DOCUMENTOS FÍSICOS

Documentos físicos contendo informações restritas ou confidenciais deverão ser armazenados de forma a impedir acesso não autorizado.

Deverão ser observados:

- **controle de acesso** - Consiste na implementação de barreiras físicas e lógicas que restringem a consulta e a circulação de documentos sigilosos exclusivamente a servidores e colaboradores autorizados através da manutenção de pastas e arquivos em salas trancadas ou armários com chave, uso de crachás de identificação para entrada no setor de arquivo, registro formal em livro de carga/sistema ao retirar ou devolver um documento, e proibição de circulação de pessoas não autorizadas nos locais de custódia;
- **organização** - Trata-se da estruturação, ordenação e catalogação sistemática do acervo físico segundo o plano de classificação do órgão com identificação clara de pastas, caixas box e armários com etiquetas explicativas, padronização na ordenação dos dossiês (por número de processo, CPF do segurado ou cronologia) e manutenção da mesa limpa ao final do expediente para evitar a exposição inadvertida de dados;
- **proteção contra extravio** - Envolve a adoção de medidas preventivas para rastrear o paradeiro das informações e evitar perdas, furtos, roubos ou desvios de documentos físicos com protocolo obrigatório para envio e recebimento de documentos entre setores ou órgãos externos, auditorias periódicas e inventários de acervo, proibições de retirada de processos originais sem autorização formal e canalização de fluxos de transporte em envelopes lacrados e identificados;
- **proteção contra danos físicos** - Refere-se ao conjunto de boas práticas de conservação preventiva e gestão ambiental para preservar o suporte físico (papel) contra degradação natural, acidentes ou sinistros instalando extintores de incêndio adequados e detectores de fumaça, controle de umidade e temperatura nos depósitos de arquivo, proteção contra incidência direta de luz solar, afastamento do acervo de tubulações de água e prevenção contra pragas urbanas (como cupins e traças);
- **descarte seguro** - Processo pelo qual os documentos que já cumpriram suas funções administrativas e prazos legais são destruídos de forma irreversível, garantindo que as informações não possam ser recuperadas ou recompostas por terceiros através da utilização de fragmentadoras de papel de alta segurança (corte em partículas);
- **observância dos prazos de guarda** - Cumprimento rigoroso da Tabela de Temporalidade de Documentos (TTD) do órgão ou da Administração Pública, que determina o tempo exato em que cada tipo de documento deve ser mantido na fase corrente, intermediária e sua destinação final (guarda permanente ou eliminação) realizando consulta à TTD antes de arquivar ou descartar qualquer processo, separação periódica de documentos que já

atingiram o tempo limite de retenção e preservação definitiva daqueles que possuem valor histórico, probatório ou permanente para o IPREV.

13. DOCUMENTOS DIGITAIS

Documentos digitais deverão ser armazenados em locais institucionais autorizados.

Sempre que aplicável, deverão existir mecanismos para:

- **controle de acesso** - Consiste na aplicação de permissões lógicas para garantir que o acesso aos documentos digitais seja concedido estritamente com base na necessidade de trabalho (*princípio do menor privilégio*) com a definição de permissões por perfil ou função (ex.: apenas leitura, edição ou exclusão), restrição de pastas compartilhadas na rede interna ou na nuvem e bloqueio de acesso público a documentos restritos ou confidenciais;
- **identificação de usuários** - Mecanismos que asseguram a individualização e autenticação de quem acessa, altera, cria ou assina um documento no sistema exigindo credenciais individuais e intransferíveis (login e senha), autenticação em dois fatores (2FA), uso de certificados digitais (como ICP-Brasil) para assinatura de processos e eliminação de contas genéricas ou compartilhadas;
- **backup** - Processo automatizado e periódico de criação e armazenamento de cópias de segurança dos arquivos digitais em locais fisicamente ou logicamente distintos do servidor principal através da execução de rotinas de backup diárias ou em tempo real (locais e em nuvem), armazenamento com criptografia e retenção de cópias fora do ambiente principal (*offsite*) para proteção contra ataques como *ransomware*;
- **preservação da integridade** - Garante que o documento digital mantido no sistema permaneça exato, completo e protegido contra alterações acidentais, corrupção de arquivos ou manipulações maliciosas não autorizadas utilizando algoritmos de codificação para verificação de integridade (como funções *hash*), restrição de permissões de edição em arquivos finalizados (conversão para formato PDF) e uso de criptografia em trânsito e em repouso;
- **recuperação** - Capacidade técnica e operacional de restaurar de forma rápida, segura e sem perda de dados os documentos digitais armazenados em caso de falhas de hardware, exclusão acidental, desastres ou incidentes de segurança com definição de metas de tempo de recuperação (RTO) e limite de perda aceitável (RPO), realização frequente de testes simulados de restauração de backups e elaboração de procedimentos claros para pronta resposta a incidentes.

14. BACKUP

O IPREV deverá manter cópias de segurança dos sistemas e dados considerados essenciais.

O procedimento de backup deverá definir:

- **o que será copiado** - Classificando os dados por nível de criticidade, priorizando bancos de dados de concessão de benefícios, sistemas de folha de pagamento de aposentados, processos administrativos digitais e registros fiscais/contábeis;
- **periodicidade** - Definição do intervalo de tempo no qual os backups serão executados, com estabelecimento de estratégias combinadas, como backups diários incrementais ou diferenciais (para dados em rápida alteração) e backups semanais ou mensais completos, garantindo a menor janela de perda de dados possível;
- **responsável** - Designação clara do Administrador de Backup ou gestor da área de TI no plano de segurança da informação, estabelecendo rotinas de checagem diária e relatórios de acompanhamento para evitar que as cópias deixem de ser executadas por falha de processo;
- **local de armazenamento** - Definição dos meios físicos e lógicos onde as cópias de segurança serão depositadas, garantindo o cumprimento da regra de redundância geográfica com adoção do modelo de redundância (como a regra 3-2-1: 3 cópias, 2 mídias diferentes, 1 fora do ambiente local), utilizando servidores locais protegidos e armazenamento em nuvem governamental ou *datacenter* secundário;
- **proteção** - Uso obrigatório de criptografia de ponta a ponta nas mídias de backup (em trânsito e em repouso), controle estrito de permissões de acesso e implementação de backups imutáveis ou isolados da rede, inviabilizando que um ataque por *ransomware* alcance e criptografe as cópias;
- **procedimento de recuperação** - Documentação passo a passo e testes periódicos para garantir que, na ocorrência de um desastre ou indisponibilidade, os dados armazenados possam ser prontamente restaurados no menor tempo possível.

Sempre que tecnicamente possível, deverá existir cópia armazenada de forma segregada do ambiente principal.

15. TESTE DE RESTAURAÇÃO

Backups não deverão ser considerados eficazes apenas porque foram executados. Deverão ser realizados testes de restauração em periodicidade definida pelo responsável técnico ou fornecedor.

O teste deverá ser registrado contendo:

- data;

- sistema/dado testado;
- responsável;
- resultado;
- falhas identificadas;
- providências adotadas.

16. ATUALIZAÇÕES E PROTEÇÃO CONTRA MALWARE

Sistemas e equipamentos deverão, sempre que tecnicamente possível:

- utilizar mecanismos de proteção;
- receber atualizações;
- utilizar software autorizado;
- possuir proteção contra malware;
- ter vulnerabilidades relevantes tratadas.

Quando a manutenção for responsabilidade de fornecedor, o contrato deverá estabelecer, quando pertinente, as responsabilidades relacionadas à segurança.

17. SEGURANÇA DE REDES

A infraestrutura de rede deverá ser protegida por mecanismos compatíveis com o porte e a criticidade do ambiente.

Deverão ser observados:

- controle de acesso;
- proteção de equipamentos;
- atualização;
- senhas administrativas;
- segregação, quando necessária;
- monitoramento compatível com a capacidade institucional.

18. GESTÃO DE INCIDENTES DE SEGURANÇA

Todo incidente ou suspeita de incidente deverá ser comunicado ao responsável definido pelo IPREV.

São exemplos:

- phishing;
- malware;
- ransomware;
- vazamento de informações;
- acesso indevido;

- perda de equipamento;
- furto;
- exclusão indevida;
- indisponibilidade;
- uso indevido de credenciais;
- alteração não autorizada de informações.

19. TRATAMENTO DE INCIDENTES

O tratamento deverá seguir, sempre que aplicável, as seguintes etapas:

1. Identificação do evento.
2. Registro do incidente e das informações disponíveis.
3. Classificação e avaliação da natureza e criticidade.
4. Análise dos sistemas e informações afetados.
5. Adoção de medidas para impedir agravamento.
6. Comunicação às pessoas ou órgãos competentes, quando necessária.
7. Correção ou mitigação.
8. Restabelecimento dos serviços.
9. Encerramento do encerramento.
10. Identificação das causas.
11. Adoção de medidas para evitar recorrência.

20. PROTEÇÃO DE DADOS PESSOAIS

O tratamento de dados pessoais deverá observar a legislação aplicável, especialmente a LGPD.

O IPREV deverá buscar garantir:

- finalidade;
- adequação;
- necessidade;
- segurança;
- prevenção;
- transparência;
- responsabilização;
- controle de acesso.

O acesso aos dados deverá ocorrer de acordo com a necessidade funcional e com as atribuições do usuário.

21. RELAÇÃO ENTRE LAI, LGPD E SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação deverá harmonizar:

Transparência + Acesso à Informação + Proteção de Dados + Segurança.

A publicidade das informações públicas constitui regra, observadas as hipóteses legais de restrição, a existência de dados pessoais em determinado documento não significa automaticamente que todo o documento seja inacessível.

Quando aplicável, deverá ser avaliada a possibilidade de disponibilização da informação com proteção ou ocultação dos dados pessoais que não possam ser divulgados.

22. RESPONSABILIDADES DOS SERVIDORES E USUÁRIOS

Compete aos usuários:

- I – Cumprir esta Política;
- II – Proteger suas credenciais;
- III – Utilizar adequadamente os recursos tecnológicos;
- IV – Proteger as informações sob sua responsabilidade;
- V – Comunicar incidentes;
- VI – Participar das capacitações;
- VII – Evitar compartilhamento indevido;
- VIII – Respeitar as regras de acesso.

23. RESPONSABILIDADES DO RESPONSÁVEL PELA TECNOLOGIA

Quando houver servidor, setor ou fornecedor responsável pela tecnologia, caberá, conforme suas atribuições:

- apoiar os controles tecnológicos;
- administrar acessos;
- apoiar backups;
- acompanhar atualizações;
- apoiar tratamento de incidentes;
- manter registros;
- orientar usuários;
- comunicar riscos relevantes.

Quando os serviços forem terceirizados, essas atividades poderão ser executadas pelo fornecedor, permanecendo o IPREV responsável pela governança e fiscalização.

24. DISPOSIÇÕES FINAIS

Esta Política entra em vigor na data de sua aprovação e deverá ser divulgada aos servidores, prestadores de serviços e demais usuários abrangidos por seu escopo. O cumprimento desta Política deverá ser acompanhado por meio de evidências documentais, registros, indicadores, avaliações de risco e ações de controle.



INSTITUTO DE PREVIDENCIA DOS SERVIDORES DE JAGUARIAÍVA/PR

CNPJ Nº 72.376.916/0001-51

FONE(43)3535-9356 e-mail: ipaspmj1992@gmail.com

RUA JOSÉ DE ALENCAR, 161 – CIDADE ALTA

CEP 84.200-000 JAGUARIAÍVA – PARANA

A PSI deverá ser considerada instrumento integrante da estrutura de governança, gestão de riscos, controle interno, transparência e proteção das informações do IPREV. Os procedimentos operacionais decorrentes desta Política poderão ser detalhados em normas, manuais, instruções de trabalho, checklists e formulários específicos.

Jaguariaíva/PR, 29 de outubro de 2026.