PREVIDÊNCIA SOCIAL DO MUNICÍPIO DE QUATRO BARRAS - PREVIBARRAS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Documento de Diretrizes e Normas

PREVIBARRAS

Quatro Barras

2025 – v.2

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

A Política de Segurança da Informação (PSI) tem por finalidade reduzir o risco de vazamentos, fraudes, erros, uso indevido, sabotagens, paralisações e roubo de informações ou qualquer outra ameaça que possa prejudicar os sistemas de informação, os recursos de processamento da informação, ou os equipamentos da Previdência Social do Município de Quatro Barras - PREVIBARRAS, fundamentada nos princípios da confiabilidade, responsabilidade, disponibilidade, integridade, confidencialidade, autenticidade, legalidade e ética.

As normativas descritas a seguir obedecem a um rigoroso processo de aplicação de regras para manter a confidencialidade, a integridade e a disponibilidade dos equipamentos e softwares, garantindo que as informações não sejam alteradas ou perdidas e que estejam disponíveis quando necessário.

As informações estão sob responsabilidade da PREVIBARRAS, buscando atender as demandas da ISO/IEC 27002:2022 sobre as regras de boas práticas para a gestão de segurança da informação com base nas regulamentações da Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018), que estabelece as formas de tratamento de dados de entidades e pessoas.

Este documento ainda apresenta informações acerca de como as atualizações devem ser aplicadas e mantidas como uma medida de boas práticas, estabelecendo diretrizes para a proteção de ativos, prevenção e responsabilidades.

2. PROCESSO DE ALTERAÇÕES

As alterações podem ser aplicadas a qualquer momento, seguindo as condições de execução contidas na tabela **CICLO DE APROVAÇÃO**. Quando os pontos apontados para mudanças forem informados e discutidos com os demais colaboradores a aplicação de atualização deverá ser modificada na tabela **CONTROLE DE VERSÃO**.

2.1 Objetivo

O objetivo principal da Política de Segurança da Informação é garantir a aplicação das três principais normas da segurança da informação:

- **Confidencialidade:** Propriedade que estabelece que a informação deva estar acessível apenas para pessoas autorizadas;
- **Integridade:** Propriedade que estabelece que a informação esteja correta, confiável, sem a ocorrência de mudanças não autorizadas;
- **Disponibilidade:** Propriedade que estabelece que a informação esteja sempre acessível para uso legítimo de pessoas autorizadas.

Com aplicação dessas diretrizes a Previdência Social do Município de Quatro Barras pode manter todas as funcionalidades exercidas pela mesma, sem nenhum risco de adversidades tecnológicas.

2.2 Classificação da Informação

As classificações das informações serão nominadas a seguir com o objetivo de sanar as condições de possíveis perdas de informações e devem ser classificadas e identificadas por rótulos para evitar vazamento de informações como senhas e acessos internos.

Ao aplicar essas condições, podem ser resolvidos de maneira prática e rápida as futuras demandas de suporte, em um curto prazo de tempo, nos seguintes níveis de informações: Pública, Interna e Confidencial.

- **Pública:** São informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio e que, por isso, não necessitam de proteção efetiva ou tratamento específico. Exemplo de informações públicas: *Editais de licitação, prestações de contas, demonstrativos de investimentos, contratos de prestação de serviços, entre outros que são abrangidas pela LAI (Lei de Acesso a Informação).*
- **Interna:** São informações de uso apenas para os servidores do instituto. Exemplos de informações internas: *Memorandos, portarias, políticas e procedimentos internos, e-mails, lista telefônica interna, avisos e campanhas internas.*

- **Confidencial:** São informações de acesso restrito ao servidor, pensionista ou aposentado e sua revelação pode violar a privacidade dos mesmos, violar acordos de confidencialidade tipo paciente e médico. Exemplos de informações confidenciais: *exames e diagnósticos de pacientes, processos judiciais, dados pessoais.*

2.3 Gestão dos Processos e da Tecnologia da Informação

A gestão dos processos e da Tecnologia da Informação requerem as seguintes ações:

- Definir as Regras de Hardware e Software e suas respectivas políticas de senhas;
- Garantir segurança física e lógica do datacenter local ou remoto;
- Garantir o correto uso das estações trabalho;
- Disponibilizar o uso seguro dos equipamentos particulares;
- Definir as regras de uso da Rede (Intranet e Internet);
- Gerenciar as padronizações de emails e seus usos comuns;
- Gerir os equipamentos de produção (impressoras e scanners);
- Manter e monitorar metodologias de back-up e armazenamentos.

2.4 Responsabilidades

- Servidores efetivos, comissionados, conselheiros e integrantes do comitê de investimentos: utilizar os recursos institucionais de forma ética, manter sigilo das informações e zelar por suas credenciais de acesso.
- Terceirizados e estagiários: cumprir as mesmas regras aplicáveis aos servidores, respeitando a confidencialidade das informações acessadas.
- Prestadores de serviços de TI: executar rotinas de backup, segurança e manutenção, mantendo sigilo sobre os dados e incidentes de que tiverem conhecimento.
- Gestores de área: monitorar o cumprimento desta política por suas equipes e comunicar eventuais violações.

- Presidência da PREVIBARRAS: aprovar, revisar e atualizar esta política periodicamente.

2.5 Gestão Processos e Pessoas

Cabe aos gestores da PREVIBARRAS a gestão dos processos da seguinte forma:

- Aprovar a Política de Segurança da Informação e suas atualizações;
- Cumprir e se fazer cumprir a presente Política;
- Ter postura exemplar em relação à segurança da informação;
- Na fase de contratação e formalização dos contratos, dar ciência à responsabilidade do cumprimento da Política de Segurança da Informação;
- Exigir assinatura do termo de confidencialidade aos parceiros, prestadores de serviços e outras entidades externas;
- Sempre que necessário informar as atualizações referentes a processos da Política de Segurança da Informação;
- No que se refere o descumprimento dos processos da Política de Segurança da Informação deve-se tomar as decisões administrativas cabíveis.

2.6 Uso de Recursos Tecnológicos

O uso da internet, correio eletrônico, computadores e demais recursos tecnológicos deve restringir-se a fins institucionais. É vedado:

- o compartilhamento de logins e senhas;
- a instalação de softwares sem autorização da área de TI;
- a utilização de recursos para fins ilícitos, pessoais ou alheios às atividades institucionais;
- o uso do e-mail institucional para comunicações não relacionadas às atividades da Autarquia.

2.7 Procedimentos de Contingência e Backup

Serão realizadas cópias de segurança (backups) diários dos sistemas informatizados e bancos de dados da PREVIBARRAS.

As cópias serão armazenadas em ambiente seguro, com verificação de integridade.

Em caso de falha de sistema, perda de dados, ataque cibernético ou incidente de segurança, será acionado o Plano de Contingência, que prevê:

- restauração imediata a partir do backup mais recente;
- comunicação ao responsável pela área de TI;
- registro do incidente e das medidas corretivas adotadas.

O fluxo detalhado dos procedimentos encontra-se descrito no Manual de Contingência de TI (Anexo I).

2.8 Controle de Acesso

- Acesso físico: o ingresso em áreas restritas (sala de servidores, arquivo físico de segurados e documentos sensíveis) será controlado pelo Setor Administrativo.
- Acesso lógico: o gerenciamento de usuários e permissões em sistemas será de responsabilidade da área de TI, incluindo criação, alteração e exclusão de acessos.
- Todos os acessos devem ser individuais, pessoais e intransferíveis.

2.9 Manualização e Mapeamento de Procedimentos

A PREVIBARRAS manterá manuais atualizados contendo o passo a passo dos principais procedimentos de segurança da informação, incluindo:

- Procedimento de backup e restauração (Anexo II);
- Procedimento de controle de acesso físico (Anexo III);
- Procedimento de controle de acesso lógico (Anexo IV);
- Procedimento para resposta a incidentes de segurança (Anexo V).

Esses documentos serão revisados sempre que necessários e disponibilizados às áreas responsáveis.

2.10 Atualização da Política

A presente política será revisada sempre que houver alteração relevante na legislação, nos sistemas utilizados ou nos processos internos, sob responsabilidade da Presidência da PREVIBARRAS em conjunto com a área de Tecnologia da Informação.

3. CONSIDERAÇÕES FINAIS

A PSI tem por objetivo preservar a disponibilidade, integridade, confidencialidade, autenticidade e salvaguarda das informações geradas, processadas e armazenadas no âmbito do Instituto, mediante o estabelecimento e difusão de diretrizes e princípios para a PREVIBARRAS, orientando quanto ao uso adequado da informação de sua propriedade.

O cumprimento desta Política e de suas normas complementares deverá ser avaliado periodicamente pelos gestores do instituto, bem como observada pelos servidores da PREVIBARRAS e membros dos órgãos colegiados.

Ressalta-se que toda a informação criada ou custodiada que for manuseada, armazenada, transportada ou descartada pelos agentes públicos ou privados vinculados ao RPPS no exercício de suas atividades, é de propriedade do PREVIBARRAS e será protegida.

Quatro Barras, 25 de setembro de 2025.

ELLEN CORREA WANDEMBRUCK LAGO:04298059936
Assinado digitalmente por ELLEN CORREA WANDEMBRUCK LAGO:04298059936
Data: 29/September/2025

ELLEN CORRÊA WANDEMBRUCK LAGO

Presidente da PREVIBARRAS

ANEXO I

PLANO DE CONTINGÊNCIA DE TI

Objetivo: definir procedimentos a serem seguidos em caso de falha, indisponibilidade ou incidente de segurança nos sistemas da PREVIBARRAS.

1. Cenários de contingência:

a) Falha de sistema
b) Perda de dados
c) Ataque cibernético
d) Indisponibilidade física

2. Procedimentos imediatos:

a) Identificação e registro do incidente pela área de TI.
b) Comunicação imediata à Presidência.
c) Adoção das medidas de contenção.
d) Restauração dos sistemas a partir do backup mais recente.

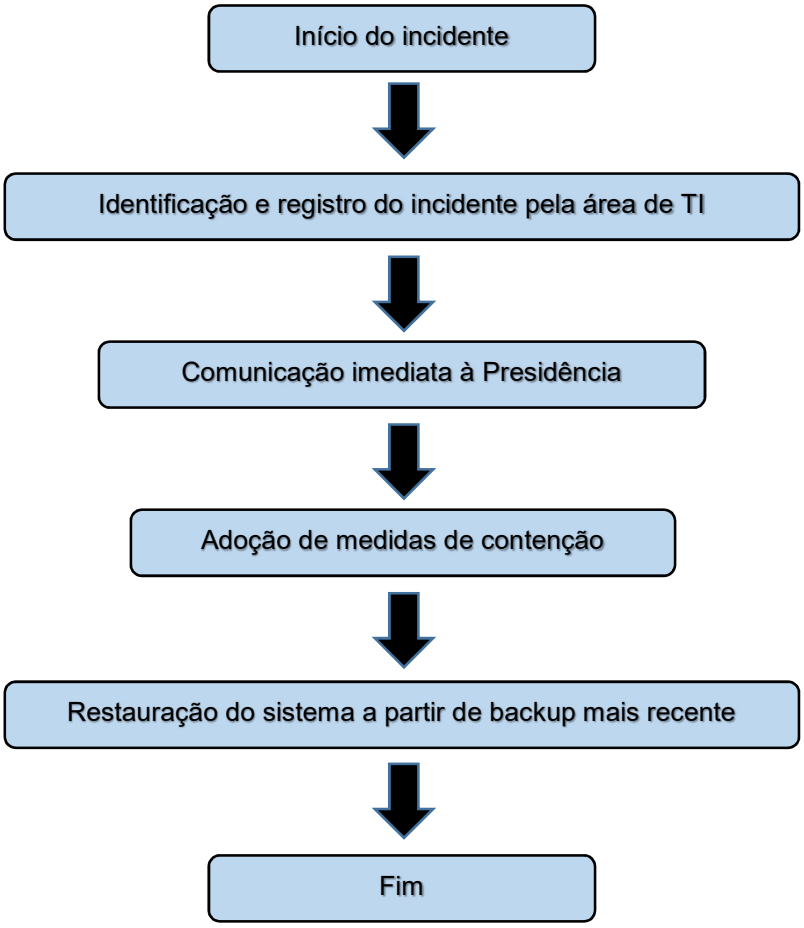
3. Responsáveis:

a) Área de TI
b) Setor Administrativo
c) Presidência

4. Prazos de resposta:

a) Notificação inicial: até 2 horas
b) Contenção: até 4 horas
c) Restauração: até 24 horas

MAPEAMENTO DO PLANO DE CONTINGÊNCIA DE TI



ANEXO II

PROCEDIMENTO DE BACKUP

Objetivo: assegurar a integridade e disponibilidade das informações por meio de cópias de segurança regulares.

1. Periodicidade:

a) Backup diário

2. Armazenamento:

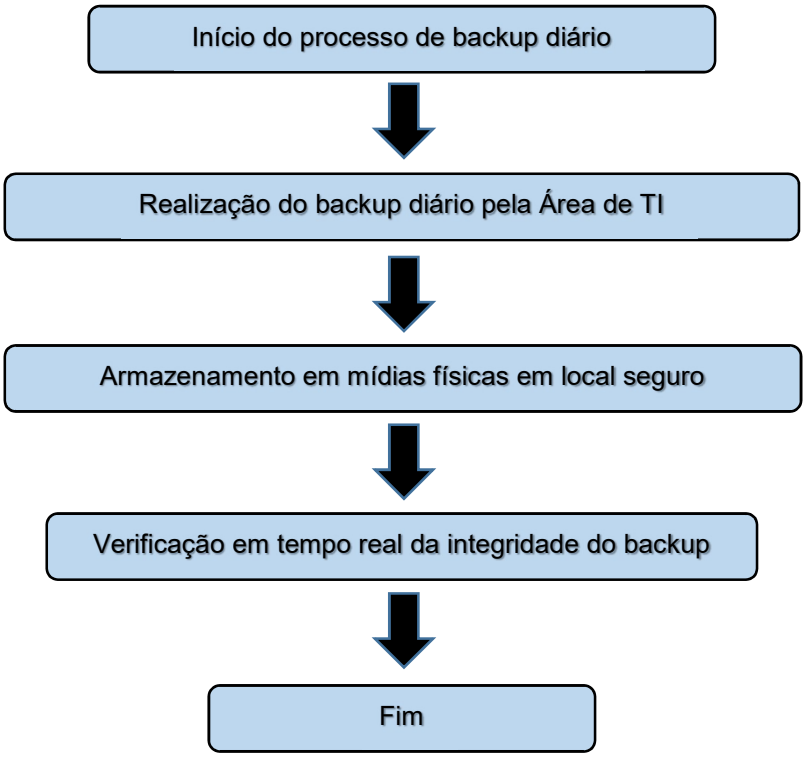
a) Mídias físicas em local seguro

3. Verificação:

a) Em tempo real

4. Responsável: Área de TI

MAPEAMENTO DO PROCEDIMENTO DE BACKUP



ANEXO III

CONTROLE DE ACESSO FÍSICO

Objetivo: garantir que apenas pessoas autorizadas acessem áreas restritas.

1. Áreas restritas:

a) Sala de servidores

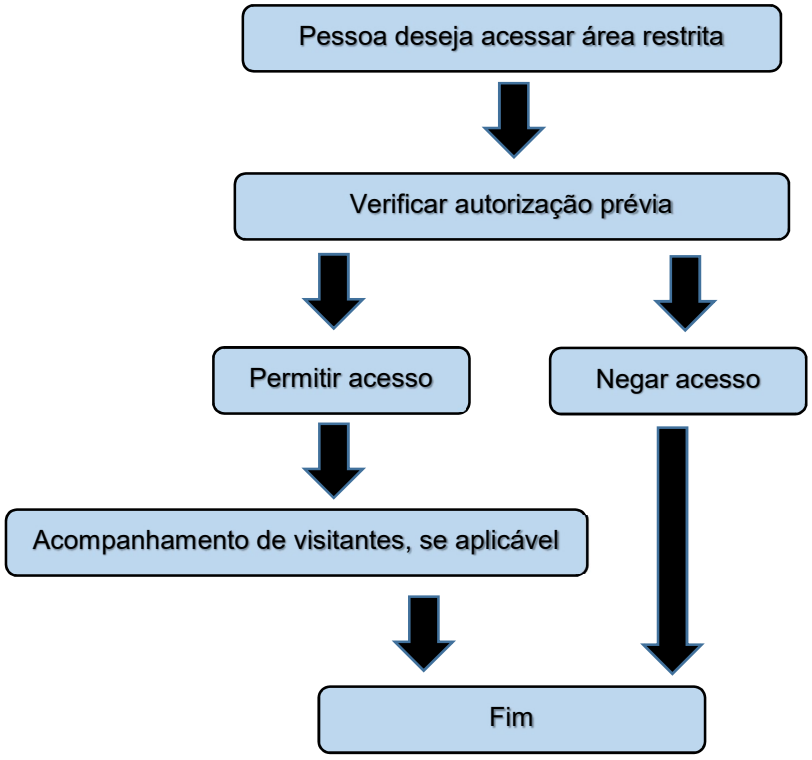
b) Arquivo físico

2. Procedimentos:

a) Entrada mediante autorização prévia

b) Acompanhamento de visitantes

MAPEAMENTO DO CONTROLE DE ACESSO FÍSICO



ANEXO IV

CONTROLE DE ACESSO LÓGICO

Objetivo: regulamentar a criação, manutenção e exclusão de usuários em sistemas.

1. Regras gerais:

a) Credenciais individuais

b) Acesso conforme função

c) Troca de senha periódica

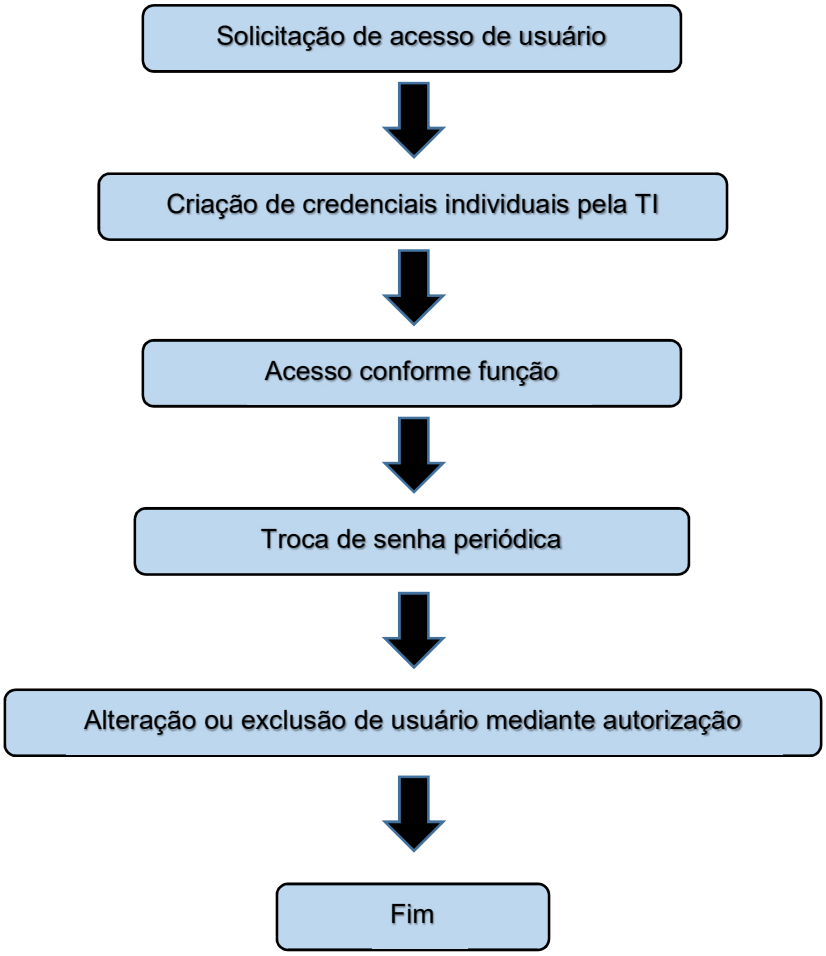
2. Procedimentos:

a) Criação mediante solicitação

b) Alteração com autorização

c) Exclusão imediata no desligamento

MAPEAMENTO DE CONTROLE DE ACESSO LÓGICO



ANEXO V

RESPOSTA A INCIDENTES DE SEGURANÇA

Objetivo: definir o fluxo de comunicação e ação diante de incidentes de segurança da informação.

1. Exemplos de incidentes:

a) Acesso não autorizado
b) Vazamento de informações
c) Infecção por vírus
d) Tentativa de fraude

2. Procedimentos:

a) Registrar o incidente
b) Comunicar à TI e Presidência
c) Avaliar impacto
d) Executar ações corretivas
e) Elaborar relatório

3. Responsáveis:

a) Área de TI (execução técnica)
b) Presidência (decisões estratégicas)

MAPEAMENTO DE RESPOSTA A INCIDENTES DE SEGURANÇA