MANUAL DO PROCESSO DE CONTINGÊNCIA V.01-2025

DIRETORIA EXECUTIVA

1. Objetivo do Plano de Contingência 🎯

Com base na Política de Segurança da Informação (PSI), o Manual de Planos de Contingência do Instituto de Previdência Social dos Servidores do Município de Açailândia - IPSEMA, tem como objetivo, Garantir a **disponibilidade** e a **integridade** das informações e sistemas informatizados do **IPSEMA** por meio de cópias de segurança (backup) eficazes e controladas, além de estabelecer regras claras para o controle de acesso (físico e lógico) a esses ativos.

---

2. Documentos Complementares

- Política de Segurança da Informação (**PSI**).

---

3. Responsabilidades e Áreas Envolvidas 👥

Abaixo, estão detalhadas as responsabilidades relativas a este procedimento, baseadas no Manual de Elaboração de Planos de Contingência e na PSI.

Quem Participa	Responsabilidades
Área de TI (Setor de TI)	Elaborar, implantar e monitorar as estratégias de contingência, planos de recuperação de informações e backup. É a **área responsável** pela execução técnica e controle das cópias de segurança.
Diretoria Executiva	Analisar e aprovar os planos de contingência e monitorar a execução.
Colaboradores	Cumprir as regras estabelecidas na PSI e comunicar incidentes. ZELAR pelos ativos de informação (físicos e digitais) e MANTER SIGILO.

4. Detalhamento do Processo: Cópia de Segurança e Recuperação (Backup) 💾

Este procedimento detalha as etapas de garantia das cópias de segurança e sua recuperação, sendo o **Setor de TI** o principal responsável pela sua execução e monitoramento.

Etapa	Atividade	Responsável	Detalhamento
1	**Solicitar** elaboração de planos de contingência das informações.	Solicitante	Inicia o processo de garantia da segurança das informações.
2	**Elaborar** estratégias de contingências (incluindo a rotina de backup).	Setor de TI	Definir o que, quando e onde será feito o backup, garantindo a **integridade** e **disponibilidade**.
3	**Analisar** e **Aprovar** planos de contingência.	Diretoria Executiva	Aprovação formal das estratégias e recursos.
4	**Aplicar** planos de recuperação de informações e backup.	Setor de TI	Execução das rotinas de backup e testes periódicos de restauração. Armazenamento seguro das mídias.
5	**Monitorar** execução do plano.	Setor de TI	Acompanhar a execução das rotinas e o estado dos backups para garantir o cumprimento.

Fluxograma do Processo: Tecnologia da Informação – Planos de Contingências

5. Controle de Acesso 🔒

O controle de acesso abrange a segurança física dos ativos e a segurança lógica dos sistemas e dados.

5.1. Controle de Acesso Lógico

O **Setor de TI** é o responsável por implantar e gerenciar os sistemas que garantem o controle de acesso lógico.

- **Identificação e Senha:** É obrigatória a identificação e senha **exclusiva** para acesso aos recursos tecnológicos do **IPSEMA**.

- **Proibição de Compartilhamento:** É **proibido** o compartilhamento de login/senha entre colaboradores.

- **Responsabilidade do Usuário:** Cada usuário é responsável pela memorização e proteção de sua senha, bem como por quaisquer danos causados em decorrência da não obediência às normas.

- **Monitoramento:** O **IPSEMA** pode implantar sistemas de monitoramento (estações, servidores, e-mail, internet) para identificar usuários, acessos e material manipulado, visando garantir a PSI.

5.2. Controle de Acesso Físico

O controle de acesso físico visa proteger os ativos, como servidores e mídias de backup, que armazenam as cópias de segurança.

- **Responsabilidade Geral:** Colaboradores devem **zelar pelos ativos de informação físicos** (processos, documentos, etc.).
- **Proteção do Ambiente:** O **Setor de TI** é responsável por instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança dos perímetros de acesso e a guarda segura de equipamentos.
- **Inspeção:** O **IPSEMA** pode realizar, a qualquer tempo, **inspeção física** nos equipamentos de sua propriedade.

6. Detalhamento do Procedimento de Contingência

1. Rotinas de Cópia de Segurança (Backup) e Recuperação

O objetivo principal das rotinas de backup é garantir a **Disponibilidade** e a **Integridade** das informações do IPSEMA.

Aspecto	Detalhamento	Área Responsável
Escopo do Backup	Deve abranger todos os **ativos de informação digitais** críticos do RPPS, incluindo bancos de dados, sistemas informatizados e arquivos eletrônicos.	Setor de TI
Princípios de Segurança	As estratégias de backup devem proteger as informações contra **alterações indevidas, intencionais ou acidentais** (Integridade). O acesso às mídias de backup deve ser obtido **somente por pessoas autorizadas** (Confidencialidade).	Setor de TI
Rotina e Frequência	O Setor de TI deve **elaborar** estratégias de contingências e **aplicar** planos de recuperação[5555]. A rotina deve incluir backups periódicos (frequência a ser definida pelo TI e aprovada pela Diretoria, por exemplo, diária, semanal) e testes de restauração para garantir a **Disponibilidade** da informação.	Setor de TI
Armazenamento	As mídias de backup devem ser armazenadas de forma segura, com controle de acesso **físico** restrito, em local distinto dos equipamentos originais, para proteção contra danos localizados (incêndio, falha elétrica, etc.).	Setor de TI
Monitoramento	O Setor de TI deve **monitorar** a execução do plano de contingência para garantir que os backups estão sendo realizados e concluídos com sucesso.	Setor de TI

2. Política de Senhas e Controle de Acesso Lógico

O controle de acesso lógico é fundamental para preservar a **Confidencialidade** das informações. O Art. 16 da PSI estabelece as diretrizes para a identificação e controle de acesso aos recursos tecnológicos do IPSEMA.

Requisito	Detalhamento	Responsável
Obrigatoriedade	É exigida a utilização de **identificação e senha exclusiva** de cada colaborador para o acesso aos recursos tecnológicos.	Colaborador / Setor de TI
Uso Pessoal e Inviolável	É **proibido o compartilhamento** de login entre os colaboradores.	Colaborador
Primeiro Acesso	Recomenda-se, como boa prática de segurança, que o usuário seja direcionado a **trocar imediatamente a sua senha** no primeiro acesso ao ambiente de rede local.	Setor de TI
Guarda e Proteção	É de **responsabilidade de cada usuário** a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.	Colaborador
Alteração em Caso de Suspeita	Os usuários podem alterar a própria senha e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram **acesso indevido** ao seu login/senha.	Colaborador
Monitoramento de Acessos	O IPSEMA poderá implantar sistemas de monitoramento nas estações de trabalho e rede para identificar usuários e respectivos acessos efetuados.	Setor de TI

INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES DO MUNICÍPIO DE AÇAILÂNDIA-IPSEMA, EM 14 DE NOVEMBRO DE 2025.

Aprovado por:

Josane Maria Sousa Araújo
Presidente do IPSEMA

Daniela Abreu Carvalho
Diretora Administrativa

Cleones Guedes da Silva
Procurador jurídico

Artur Henrique Magalhães Costa
Diretor Financeiro

Raimundo Fonseca Santos
Controlador Interno