MANUAL DE SEGURANÇA DA INFORMAÇÃO

CAAPSML – Caixa de Assistência, Aposentadoria e Pensões dos Servidores Municipais de Londrina

V.12/2025.

1. INTRODUÇÃO

A Segurança da Informação na CAAPSML tem como objetivo proteger os ativos de informação, assegurar a continuidade dos serviços previdenciários, mitigar riscos operacionais e garantir conformidade às legislações aplicáveis, incluindo a LGPD, normativas municipais e diretrizes de governança.

A infraestrutura de TI utilizada pela CAAPSML é disponibilizada pela Prefeitura Municipal de Londrina (PML), notadamente pela Diretoria de Tecnologia da Informação (DTI), sendo complementada pelos serviços prestados pelas empresas fornecedoras de sistemas.

Este manual consolida os processos de: (i) cópias de segurança (backup); (ii) controle de acesso físico; (iii) controle de acesso lógico aos sistemas corporativos e integra o conjunto de Procedimentos Padrão da CAAPSML.

2. REGULAMENTAÇÃO UTILIZADA

- Lei Geral de Proteção de Dados – LGPD (Lei Federal nº 13.709/2018);
- Política Municipal de Segurança da Informação – Portaria nº 111/2025;
- Decreto nº 275, de 05 de março de 2020.

3. OBJETIVO

Estabelecer diretrizes, responsabilidades e procedimentos para:

- Realização de backups e retenção de dados;
- Controle de acesso físico às dependências;
- Concessão, alteração e cancelamento de acessos aos sistemas corporativos utilizados pela CAAPSML;
- Garantir a integridade, confidencialidade e disponibilidade das informações.

4. RESPONSABILIDADES

Atividade	DTI – PML	Empresas Fornecedoras
Backup dos sistemas e bancos de dados	x	x
Controle de acesso físico	x	x
Concessão de acesso à rede corporativa	x	
Concessão de acesso ao sistema previdenciário		x

5. MANUALIZAÇÃO DAS ATIVIDADES

5.1 PROCESSO DE CÓPIAS DE SEGURANÇA DE SISTEMAS E BANCO DE DADOS

5.1.1 Backup realizado pela Prefeitura Municipal de Londrina – DTI

- Periodicidade: diária, semanal e mensal;
- Agendamento: automático;
- Mídia: infraestrutura corporativa da DTI (storage, soluções cloud).

5.1.1.1 Tempo de Retenção

- Backup diário: últimos 15 dias;
- Backup semanal e mensal: últimos 45 dias.

5.1.1.2 Armazenamento

Backups são armazenados em ambiente seguro, com controle de acesso e redundância, garantindo recuperação em caso de contingência.

5.1.1.3 Processo de controle de acesso físico

- Crachá funcional e credenciais de acesso são pessoais e intransferíveis;
- Ambientes críticos (arquivo, sala de CPD) têm acesso restrito;
- Setores devem comunicar imediatamente desligamentos para revogação de acessos.

5.1.2 Backup dos sistemas fornecidos por empresas terceirizadas

Os dados da CAAPSML hospedados na plataforma da empresa Actuary *(locação de Software de Gestão Integrada de Regime Próprio de Previdência Social*) utilizam infraestrutura de nuvem de alta segurança operada pela Oracle Brasil, com padrões Tier IV e certificações internacionais. Os principais elementos da infraestrutura incluem:

a) Estrutura física e redundância

- Data Center principal localizado em São Paulo – SP;
- Replicação integral e contínua para Data Center secundário em Vinhedo – SP;
- Arquitetura de alta disponibilidade com redundância geográfica;
- Certificações internacionais: ISO 27001, SOC 1, SOC 2, PCI DSS e outras aplicáveis.

b) Controles de acesso físico

- Autenticação biométrica avançada (impressão digital e reconhecimento facial);
- Cartões criptografados e senhas fortes;
- Acesso restrito exclusivamente a pessoal autorizado;
- Múltiplas camadas de verificação desde o perímetro até as salas de servidores.

c) Gestão de concessão, alteração e revogação de acessos

- Segue o princípio do menor privilégio;
- Concessão condicionada à finalidade e aprovação hierárquica;
- Revogação imediata e auditável;
- Acesso de terceiros sempre supervisionado e registrado.

d) Registro e monitoramento de acessos (logs)

- Registros completos de data, hora, identidade, área acessada e duração;
- Monitoramento 24h/7 por equipes de segurança;
- Alertas automáticos de tentativas de acesso não autorizado.

e) Sistema de câmeras e vigilância

- Cobertura total das áreas críticas do Data Center;
- Imagens criptografadas e armazenadas conforme política interna;
- Acesso restrito somente a pessoal autorizado.

f) Detecção e combate a incêndio

- Detectores de fumaça (pontuais e por aspiração) e de calor;
- Sistemas de supressão com agentes limpos (FM-200, Novec 1230);
- Testes e manutenções regulares.

g) Controle de temperatura e umidade

- Climatização de precisão (HVAC) com redundância;
- Sensores contínuos com alarmes;
- Monitoramento ambiental permanente.

h) Barreiras físicas

- Paredes reforçadas e portas com múltiplos pontos de travamento;
- Vidros blindados/laminados;
- Perímetro protegido com cercas, barreiras veiculares e vigilância armada.

i) Energia e continuidade operacional

- UPS/Nobreaks em configuração redundante (N+1 ou 2N);
- Geradores de alta capacidade com autonomia para dias de operação;
- Testes de carga e simulações de falha elétrica.

j) Proteção contra surtos e picos de energia

- Dispositivos DPS em múltiplos níveis;
- Aterramento robusto;
- Filtragem elétrica para proteção dos equipamentos.

5.1.2.2 Rotina de Backup

- Procedimentos de contingência: consistem na realização de backup diário do banco de dados e na execução de cópias das máquinas virtuais hospedadas nos ambientes de cloud contratados pela Actuary, garantindo restauração completa em caso de falhas ou indisponibilidade.
- Replicação para Data Centers redundantes: o backup é executado diariamente junto ao Data Center da Oracle Brasil, localizado em São Paulo/SP, com replicação simultânea para unidade redundante em Vinhedo/SP. O serviço é prestado mediante contrato específico que prevê o fornecimento de infraestrutura em nuvem para armazenamento seguro dos dados e hospedagem das aplicações desenvolvidas pela Actuary. Isso garante que todos os dados permaneçam sincronizados em dois ambientes físicos distintos, reforçando a continuidade operacional.
- Backup complementar na Actuary: além da redundância Oracle, uma cópia diária adicional é replicada para o Data Center próprio da Actuary, localizado em Curitiba/PR, ampliando a camada de proteção e recuperação em contingências.

- Retenção mínima: backups armazenados por período mínimo de 90 dias, conforme política técnica da fornecedora.
- Responsabilidade técnica: toda a execução, monitoramento, segurança e restauração dos backups ficam sob responsabilidade da Actuary, conforme previsto contratualmente.

5.3 PROCESSO DE CONCESSÃO DE ACESSO AOS SISTEMAS

5.3.1 Acesso lógico aos sistemas da PML (Rede/DTI)

5.3.1.1 Solicitação de Acesso

- Realizada via SEI pelo gestor da unidade;
- A DTI cria/atualiza contas conforme permissões solicitadas;
- Perfis são definidos segundo as atividades do servidor.

5.3.1.2 Política de Senhas

- Mínimo 8 caracteres;
- Uso de letras, números e caracteres especiais.

5.3.1.3 Bloqueio e Cancelamento

A conta será bloqueada por:

- Suspensão ou desligamento;
- Solicitação do gestor

5.3.1.4 Obrigações do Usuário

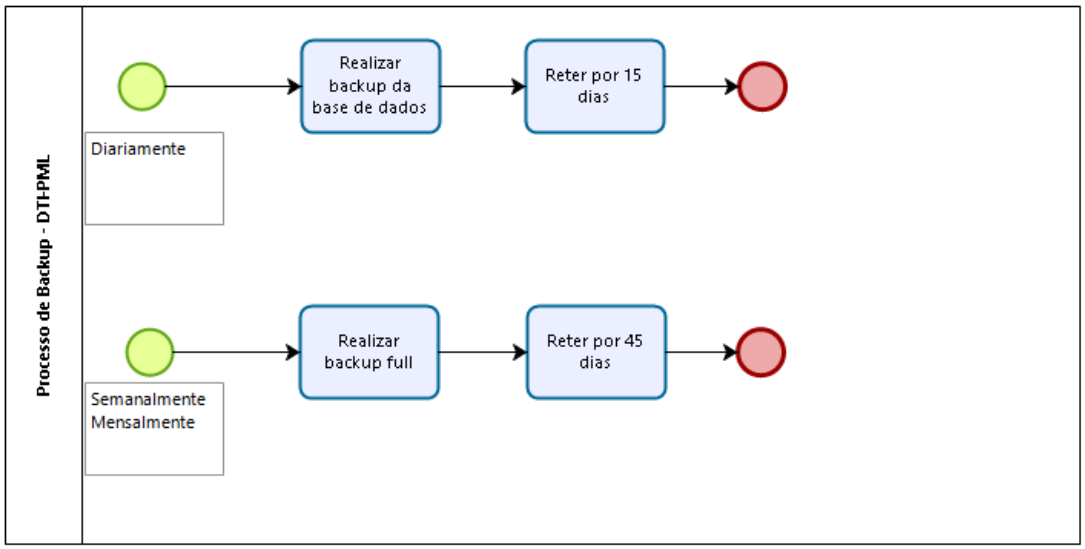
- Não compartilhar senhas;
- Bloquear estação ao ausentar-se;
- Reportar incidentes à DTI;
- Utilizar sistemas apenas para fins institucionais.

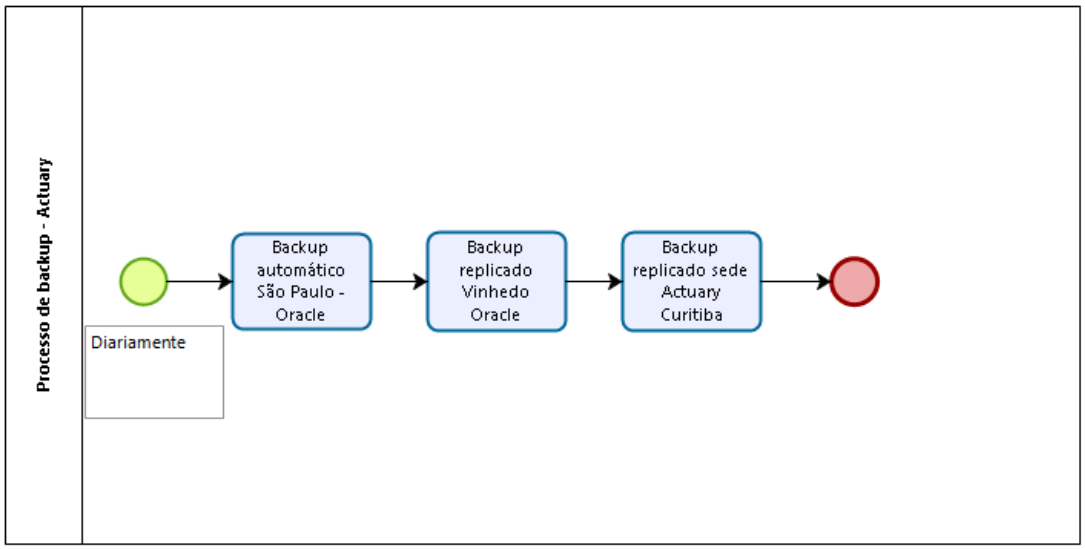
5.3.2 Acesso ao sistema previdenciário

- Setor demandante solicita aos gestores do Sistema, Diretoria de Benefícios Previdenciários e Gerências da Diretoria;
- A Diretoria e/ou gerências analisam permissões e perfis e encaminham à empresa contratada;
- A empresa contratada encaminha login e senha ao email do solicitante, que devem ser trocadas no primeiro acesso.
- O cancelamento deve ser realizado imediatamente após desligamento ou mudança de função.

6. FLUXOGRAMA DOS PROCESSOS

6.1 Processos de Backup





6.2 Processos de acesso a Rede e Sistemas